# Practical Free-Space Quantum Key Distribution

Philip Michael Gorman
B.Sc. (Hons), MInstP.

Thesis submitted for the degree of Doctor of Philosophy

Department of Physics
Heriot-Watt University

December 2010

# ABSTRACT

Within the last two decades, the world has seen an exponential increase in the quantity of data traffic exchanged electronically. Currently, the widespread use of classical encryption technology provides tolerable levels of security for data in day to day life. However, with one somewhat impractical exception these technologies are based on mathematical complexity and have never been proven to be secure. Significant advances in mathematics or new computer architectures could render these technologies obsolete in a very short timescale.

By contrast, Quantum Key Distribution (or Quantum Cryptography as it is sometimes called) offers a theoretically secure method of cryptographic key generation and exchange which is guaranteed by physical laws. Moreover, the technique is capable of eavesdropper detection during the key exchange process. Much research and development work has been undertaken but most of this work has concentrated on the use of optical fibres as the transmission medium for the quantum channel. This thesis discusses the requirements, theoretical basis and practical development of a compact, free-space transmission quantum key distribution system from inception to system tests. Experiments conducted over several distances are outlined which verify the feasibility of quantum key distribution operating continuously over ranges from metres to intercity distances and finally to global reach via the use of satellites.

## Acknowledgements

I would like to extend my thanks to my supervisor, Professor Gerald Buller for his encouragement, advice and help during the preparation of this thesis. Equal thanks should also be extended to my industrial supervisors, firstly Professor John G. Rarity, who got me into this in the first place, and Dr. David A. Huckridge who graciously assented to finish where JGR left off.

I would also like to thank the single photon optics team at Malvern, David Benton, David Taylor, Ewan Finlayson and last, but by no means least, the magnificent Paul Tapster. I didn't realise one could do such good work while laughing so much.

Acknowledgement should also be made to the Lasers and Photonics group at Malvern, Rebecca Wilson, David Orchard, Andrew Turner, Kevin Ridley, Terry Shepherd and the rest. They are an inexhaustible supply of know-how and advice. I should also like to acknowledge support of QinetiQ and the UKMoD for funding the work over a decade.

Finally, I would like to thank my parents, Jean and Frank (& Glen), my brothers, Andrew and Matthew and my fantastic wife, Loll.

ACADEMIC REGISTRY

# Research Thesis Submission

| | | | |
|---|---|---|---|
| Name*:* | Philip Michael Gorman | | |
| School/PGI: | School of Engineering and Physics | | |
| Version: *(i.e. First, Resubmission, Final)* | Final | Degree Sought (Award **and** Subject area) | Doctor of Philosophy (Physics) |

## Declaration

In accordance with the appropriate regulations I hereby submit my thesis and I declare that:

1) the thesis embodies the results of my own work and has been composed by myself
2) where appropriate, I have made acknowledgement of the work of others and have made reference to work carried out in collaboration with other persons
3) the thesis is the correct version of the thesis for submission and is the same version as any electronic versions submitted*.
4) my thesis for the award referred to, deposited in the Heriot-Watt University Library, should be made available for loan or photocopying and be available via the Institutional Repository, subject to such conditions as the Librarian may require
5) I understand that as a student of the University I am required to abide by the Regulations of the University and to conform to its discipline.

* *Please note that it is the responsibility of the candidate to ensure that the correct version of the thesis is submitted.*

| | | | |
|---|---|---|---|
| Signature of Candidate*:* | | Date: | |

## Submission

| | |
|---|---|
| Submitted By *(name in capitals):* | |
| Signature of Individual Submitting: | |
| Date Submitted: | |

## For Completion in Academic Registry

| | | | |
|---|---|---|---|
| Received in the Academic Registry by *(name in capitals):* | | | |
| Method of Submission *(Handed in to Academic Registry; posted through internal/external mail):* | | | |
| E-thesis Submitted (mandatory for final theses from January 2009) | | | |
| Signature: | | Date: | |

# TABLE OF CONTENTS

## List of relevant publications by the author

### *Conference papers*

**P.M. Gorman,** P.R. Tapster and J.G. Rarity, "Secure Free-space Key Exchange Over a 1.2 km Range Using Quantum Cryptography", CLEO/Europe-IQEC (10-15 September 2000).

J.G. Rarity, **P.M. Gorman,** T.E. Wall, P.R. Tapster, "Free-space quantum cryptography and satellite key uploading", International Quantum Electronics Conference, 2000, Conference Digest, (2000).

C. Kurtsiefer, P. Zarda, M. Hälder, **P.M. Gorman,** P.R. Tapster, J.G. Rarity, H. Weinfurter, "Long-distance free-space quantum cryptography", Proc. SPIE Vol. 4917 (Quantum Optics in Computing and Communications), 25-31, (2002).

J. Rarity, M. Aspelmeyer, H. Weinfurter, C. Kurtsiefer, **P.M. Gorman**, P.R. Tapster, T. Jennewein, M. Pfennigbauer, W. Leeb, A. Zeilinger, "Quantum communications in Space", in Proc. CLEO Europe, Conference on Lasers and Electro-Optics, Munich, Germany, (2003).

J.G. Rarity, **P.M. Gorman**, P.R. Knight, H. Weinfurter & C. Kurtsiefer, "Quantum communications in space", Proc. SPIE Vol. 5161 (Quantum Communications and Quantum Imaging), 240-251, (2004).

P.R. Tapster **P.M. Gorman,** D.M. Benton, D.M. Taylor and B.S. Lowans, "Developments toward practical free-space quantum cryptography", Proceedings of SPIE Vol 5815, 24, 176-179, (2005).

**P.M. Gorman**, "SPADs in practical quantum cryptography systems", Rank Prize Funds Mini symposium: Single photon detectors – Physics and applications, Grasmere 12-15th January 2009.

## *Journal papers*

J.G. Rarity, P.R. Tapster, and **P.M. Gorman, "**Free-space key exchange to 1.9 km and beyond", J. Mod. Opt. **48**, 1887–1901 (2001).

J.G. Rarity, **P.M. Gorman**, P.R. Tapster, "Secure Key Exchange over a 1.9 km Free-space Range Using Quantum Cryptography", Electron Lett **37**, p512-14, (2001).

C. Kurtsiefer, P. Zarda, M. Hälder, H. Weinfurter, **P.M. Gorman**, P.R. Tapster, and J.G. Rarity, "Quantum cryptography: A step towards global key distribution", Nature **419**, 450, (2002).

J.G. Rarity, P.R. Tapster, **P.M. Gorman** and P.R. Knight, "Ground to satellite secure key exchange using quantum cryptography", New Journal of Physics **4,** 82.1–82.21, (2002).

D.M. Benton, **P.M. Gorman**, P.R. Tapster and D.M. Taylor, "A compact free space quantum key distribution system capable of daylight operation" Optics Communications, **283**, 11, 2465-2471, (2010).

## *Poster papers*

"A compact free space quantum key distribution system capable of daylight operation", D.M. Benton, **P.M. Gorman**, P.R. Tapster and D.M. Taylor, SECOQC QKD Network Demonstration and conference, Vienna, (Oct 8-10, 2008).
(Also Photon 08, Heriot-Watt University, 2008).

## *Books*

Quantum Communications and Cryptography (Edited by Alexander V. Sergienko)
Chapter 9. Free-Space Quantum Cryptography, C. Kurtsiefer, M. Hälder, H. Weinfurter, P. Zarda, P.R. Tapster, **P.M. Gorman** and J.G. Rarity.
CRC Press 2006, Print: ISBN: 978-0-8493-3684-3.

# Chapter 1 - Introduction

## 1.1 Introduction

This thesis is primarily concerned with the practical design and implementation of free-space quantum cryptographic or quantum key distribution (QKD) technology. QKD is a relatively novel method of creating and sharing random numbers for use as cryptographic keys.

The ideas behind QKD have been expounded only within the last 40 years and practical realisations have been implemented only within the last 25. As such it is a fledgling technology which has its roots in two fairly recent formulations of physical theories, those of quantum mechanics and information theory. In fact it may be reasonably stated that quantum cryptography is the first practical application of quantum mechanics at a true single particle level [1].

Apart from being a fascinating area of study for these reasons alone, quantum cryptography has something else to offer. The security provided by quantum cryptography arises as a result of physical laws (such as Heisenberg's uncertainty principle [2], [3]) and can theoretically be proven to be absolutely secure. In contrast, contemporary, classical cryptographic systems are guaranteed, in most cases, by, for example, the mathematical complexity of so-called one-way functions [4]. Whilst suitable for most applications, this represents a weakness which could be exposed at any time in the future and thus potentially compromises any data which has been protected by classical cryptography.

## 1.2 Classical cryptography

Whilst it is not in the scope of this thesis to present an extended discussion, it is advantageous to point out some of the features and shortcomings of classical cryptography which make QKD research a worthwhile pursuit, as well as placing the use of the technology in context.

There are a lot of reasons for wanting to keep a secret and there are a lot of ways of doing it. Short of never divulging the secret, a technique of dubious practicality, it makes sense to protect the secret information in some way so as to render it intelligible only to those authorised to receive it.

It also makes sense to protect the secret in such a way as to be very sure that it never falls into the wrong hands, or at least, that if it does, it remains unintelligible for as long as matters.

Classical cryptography has been around for a long time, possibly since the development of human communication skills. Over the centuries many methods of encryption and cryptanalysis have been used and a review of these may be found in any book (for instance [5]) or internet search on the subject.

The modern era (or as some have labelled it, the information age [6], [7]), with the advent of electronic communication systems and the theory of information as a physical quantity, has seen an almost exponential growth in the amount of information exchanged. Information is seen to possess intrinsic value as well as symbolic value (such as the location of that buried treasure). To illustrate this, the figure below depicts internet usage and traffic statistics over the last 15 years.

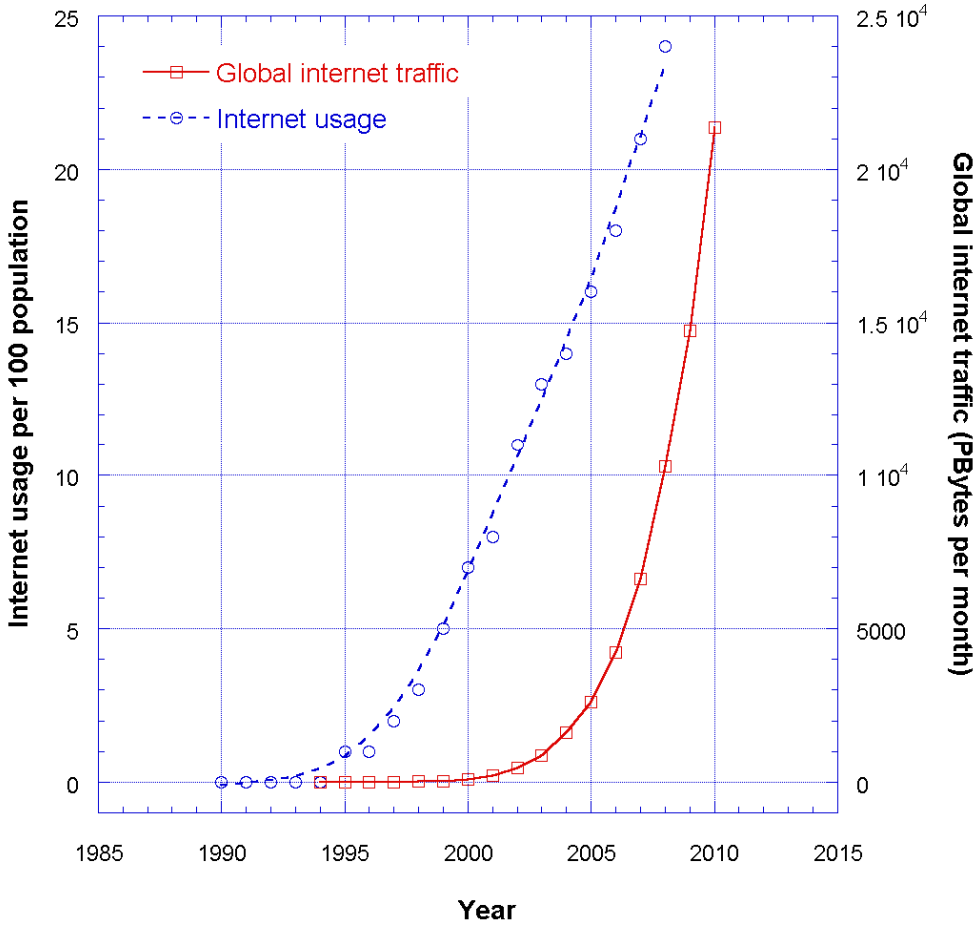


*Figure 1.1.World Internet usage per 100 population and internet traffic statistics for 1990 to 2010. Internet usage follows a quadratic relation whilst traffic is increasing exponentially. (Statistics: World Bank data catalogue [8], Cisco systems Inc).*

It is easy to see that both usage and traffic are growing at a high rate. This implies a growth in the requirement for methods of safeguarding data is necessary, not just over the internet but in all forms of communication. Classical cryptography currently provides this safeguard through several mechanisms:

- One time pad (or Vernam cipher [9])
- Private (or symmetrical) key cryptography
- Public (or asymmetrical [4]) key cryptography

The most secure form of encryption is a cipher called a one-time pad wherein a string of random data is used bit-wise to encrypt the information to be protected. The method is sometimes called the Vernam cipher after one of its inventors. The advantages of such a cipher are that it is simple and provably secure [10] providing certain criteria are met. A disadvantage is that the random number string used to encrypt the data must be as long as the plaintext to be enciphered which intensively consumes key material and therefore presents a problem for creation and distribution of keys.

A lower level of security can be provided by so-called symmetrical encryption algorithms such as the Advanced Encryption Standard (AES) with varying levels of security depending on the seed key length [11]. The seed key is single, shared key which is used as the basis for an encryption algorithm which is then used to encrypt the data. The same key is used for all data until the system is re-keyed (at certain intervals, depending on the level of security required). Symmetric key ciphers use key material more sparingly than the one-time pad but are not provably secure, being subject to a variety of attacks. Furthermore, the possession by the users of identical keys presents a problem since this requires a previous secret to have been shared by the users.

Public key cryptography was originally proposed in the mid-1970s by Martin Diffie and Whitfield Hellman and further developed by Rivest, Shamir and Adleman (although the technique was claimed to have been independently invented in 1973 by the UK government's GCHQ). In essence the encryption algorithm works by generating two different, but related, keys. A private key, which is kept secret, and a public key which is broadcast openly. Someone wishing to send a message to the private key holder then encrypts the message with the public key thus yielding a cipher which can only be read with the private key. The process takes a little longer than symmetrical cryptography but provides tolerable security for low value data transmission.

The public key method is most often used for the distribution of symmetrical keys and forms the basis for much of the data security used by the internet.

The security of public key cryptography depends on the mathematical difficulty of factorising large numbers, however, no-one has yet proved that this is, in fact, difficult. Therefore there is no guarantee that an algorithm may yet be discovered which can accomplish this factorisation easily. Moreover, with the advent of Quantum Computing, all mathematical-based encryption algorithms may become insecure in a very short space of time [12], [13].

### 1.3 Security and cryptography.

Everyone has secrets, even if the secret is just the number of a credit card PIN (of course some secrets are infinitely more dangerous). To safeguard these secrets a robust security policy must be implemented, particularly in areas such as communications where the amount, and value, of data is truly staggering. However, a robust security policy is only as strong as its weakest link. By way of example, the figure below shows some of the areas where information security is implemented and where QKD can be of service.

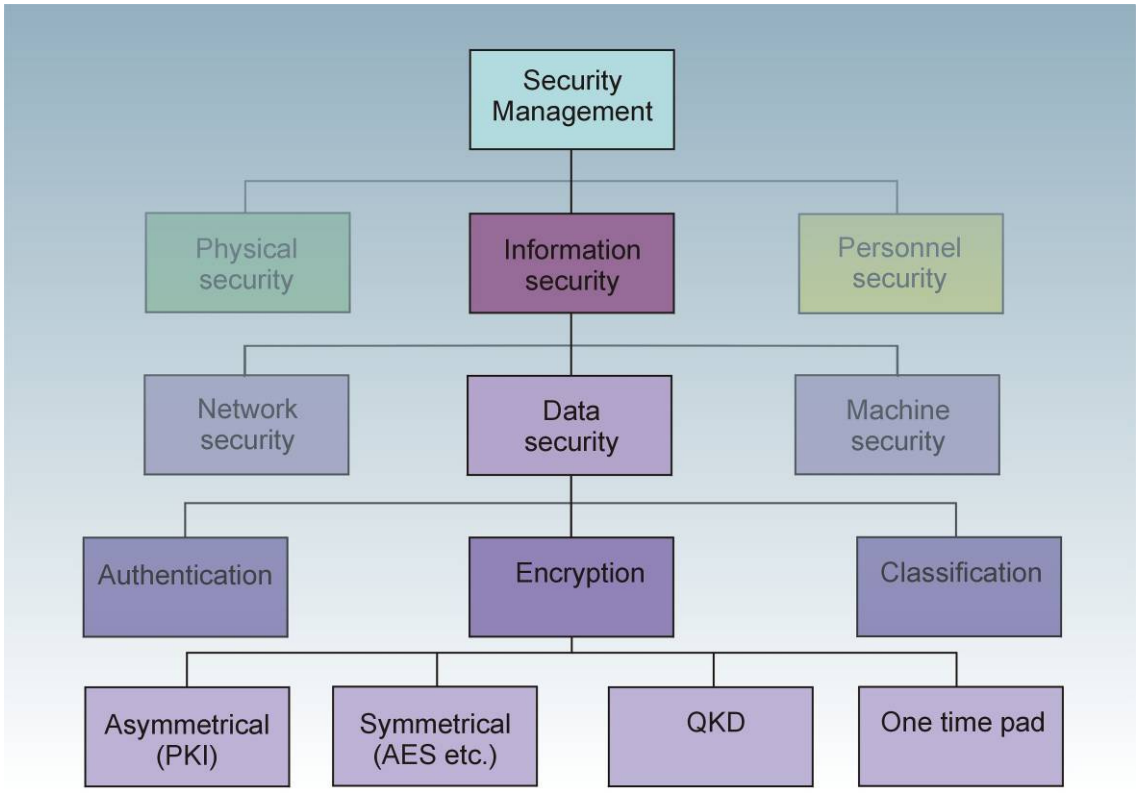


*Figure 1.2. Hierarchy of controls for a security policy. QKD has a small but important place in an overall security strategy. However robust the encryption, a security strategy can still be broken in a large number of ways.*

Quantum cryptography occupies a position where it is used, along with several other tools, to secure the data, either for storage or transmission. QKD can provide additional security in that during the key exchange process, examination of the statistics of the generated keys allows the presence of an eavesdropper to be detected.
A note of caution, however, if QKD does render stored and transmitted data unconditionally secure as is sometimes claimed then a potential eavesdropper may redirect their attack against any one of the other areas depicted in Figure 1.2.

### 1.4 Outline of this thesis

The work described in this thesis covers a decade of research and development of free-space quantum cryptography systems at QinetiQ, (formerly the Defence Research Agency at Malvern, U.K.) and culminates with the construction of a compact system capable of operating in daylight. The thesis is set out as follows:
In chapter 2, the field of QKD is reviewed from the beginning, at around 1970 with the original paper by Stephen Wiesner [14]. The chapter attempts to give a chronological discussion of some of the chief innovations in the area with a particular emphasis on technologies, both fibre and free-space.

Chapter 3 attempts to place all of the theoretical concepts required to understand the issues facing a free-space QKD system constructor into one place. The chapter starts by reviewing some Quantum mechanical concepts and continues by outlining the functional steps of the BB84 key exchange protocol and some of the attacks which could be mounted by an eavesdropper. A detailed discussion of transmission of optical radiation by various means is then given with particular emphasis on atmospheric phenomena affecting the transmission of electro-magnetic radiation. The chapter concludes with a look at random number generation and single photon counting techniques.

The idea of a Generic system is introduced in chapter 4 with the purpose of gaining an understanding of how the theory and protocols are translated into a physical realisation. A generic system is defined as the simplest method of achieving the goals set by the protocol. Not surprisingly, many systems use the same optical set-up for implementing the protocol. The chapter also serves as a benchmark, allowing comparison with some of the other technologies described in the thesis. This is also the final chapter in part 1 of the thesis, dealing with theoretical considerations.

Chapter 5 is the first practical chapter and deals with the early work in the field. Construction of a breadboard system is detailed along with details of the various system requirements and how they were implemented in a real world scenario. Throughout the chapter, constant development is seen with the resulting system used in a world record QKD experiment in the mountains of Southern Germany.

In chapter 6 it is shown how the breadboard system evolves into a much more compact and usable system with a measure of automation and portability. Several innovations and improvements to the system are discussed. The chapter continues with the analysis of several experimental runs against the state of the art security proofs provided by the theoretical experts. The final section of the chapter deals with a long range experiment in the Canary Islands where the system was part of an international collaboration exchanging keys over a distance of 144km.

In the final practical based chapter 7, the compact QKD system is fitted with redesigned electronics giving computer control over several system parameters. Several other improvements are discussed such as protocol and pointing and tracking. The system is also converted to daylight operation and the chapter culminates in a seven day trial of system performance.

Chapter 8 provides a summing up of the thesis and a brief discussion of the state of the art in the world and at QinetiQ. Some future technologies are discussed as well as some ideas for future work in the area.

## 1.5 Chapter 1 references


[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography", Reviews of Modern Physics, Volume 74, January 2002.

[2] W. Heisenberg, "Über den anschaulichen Inhalt der quantentheoretischen Kinematic und Mechanik", Zeitschrift für Physik, **43**, 172–198 (1927).

[3] W. Heisenberg, "The physical content of quantum kinematics and mechanics", pages 62–84, Princeton University Press, ISBN 0-691-08316-9 (1983).

[4] R.L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, **21** (2), 120–126 (1978).

[5] S. Singh, "The code book: the science of secrecy from ancient Egypt to quantum cryptography", Anchor Books, ISBN 0385495323 9780385495325. (2000).

[6] E.C. Lallana and M.N. Uy, "The Information Age", UNDP-APDIP, (2003).

[7] "The Information Age: An Anthology on Its Impact and Consequences", Edited by D.S. Alberts and D.S. Papp, CCRP Publication Series, (1997).

[8] The World Bank data catalogue, Internet usage statistics per 100 population. URL: http://data.worldbank.org/.

[9] G.S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications", Journal of the American Institute of Electrical Engineers, **45**, 109–115 (1926).

[10] C. Shannon, "Communication Theory of Secrecy Systems", Bell System Technical Journal **28** (4): 656–715 (1949).

[11] Federal Information Processing Standard FIPS – 197, Advanced Encryption Standard (AES), URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (2010).

[12] D. Deutsch, “Quantum theory, the Church-Turing principle and the universal quantum computer”, Proceedings of the Royal Society of London A **400**, 97-117 (1985).

[13] P.W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring”, IEEE Symposium on Foundations of Computer Science, pages124–134, IEEE, (1994).

[14] S. Wiesner, “Conjugate coding”, SIGACT News, **15** (1), 78–88 (1983).

# Chapter 2– An historical review of QKD Technology

## 2.1 Introduction

The purpose of this chapter is to explore the development of QKD technologies in a chronological context. Many of the technologies discussed also find application in the wider field of quantum information technologies (e.g. Quantum computing and quantum communications), however attempts will be made to restrict this review to those technologies having direct relevance to Quantum Key Distribution.

Although originally termed Quantum Cryptography, the technology is more accurately known as Quantum Key Distribution. However, this is still something of a misnomer since to securely exchange keys two parties must already share a secret key in order to authenticate their identities. So, in reality, the technology described within this thesis is correctly termed Quantum Key Growing or Quantum Key Expansion. However, for the rest of this thesis the term Quantum Key Distribution (QKD) shall be used.

Some of the achievements documented here are built on earlier work and where this is the case, I have referenced the earlier work after the later, but perhaps, better known, work.

## 2.2 Foundations

Quantum key distribution is built upon two of the most profound discoveries of the twentieth century, namely, the discovery and formulation of quantum mechanics and of information theory. QKD is still a relatively young technology, being first proposed in 1970 [1] and first demonstrated in 1989 [2]. It is fascinating to be able to observe the evolution of a new technological field from emergence through to practical applications and commercial exploitation.

Many of the developments in the history of QKD were not aimed specifically at QKD but rather at the burgeoning experimental realisations of quantum mechanical theory. Moreover, in common with many other technologies (for example, the field-effect transistor [3], [4], [5] and the laser [6], [7]), the theoretical description arrived decades before experimental apparatus were constructed. Complete practical realisations of the QKD theory required significant advances in several related fields before such systems became feasible.

## 2.3 The birth of QKD

The foundations of QKD were originally laid out in an article most likely written in the late nineteen sixties by a then graduate student named Stephen Wiesner studying at Columbia University. The article was entitled “Conjugate Coding”, and in it Wiesner proposed two techniques of manipulating information in a way that rendered it secure from forgery and eavesdropping [1].

The first technique was a type of “oblivious transfer” (a decade later also independently proposed by Rabin [8]) and describes a “means of transmitting two messages, either but not both of which may be received”.

Whilst the technique proposed was limited to the exchange of “two mutually exclusive messages” it explicitly mentions the use of conjugate codes to encode information and even goes so far as to propose the use of polarisation modulation to prepare the encoding of the messages for transmission through a “light pipe”.

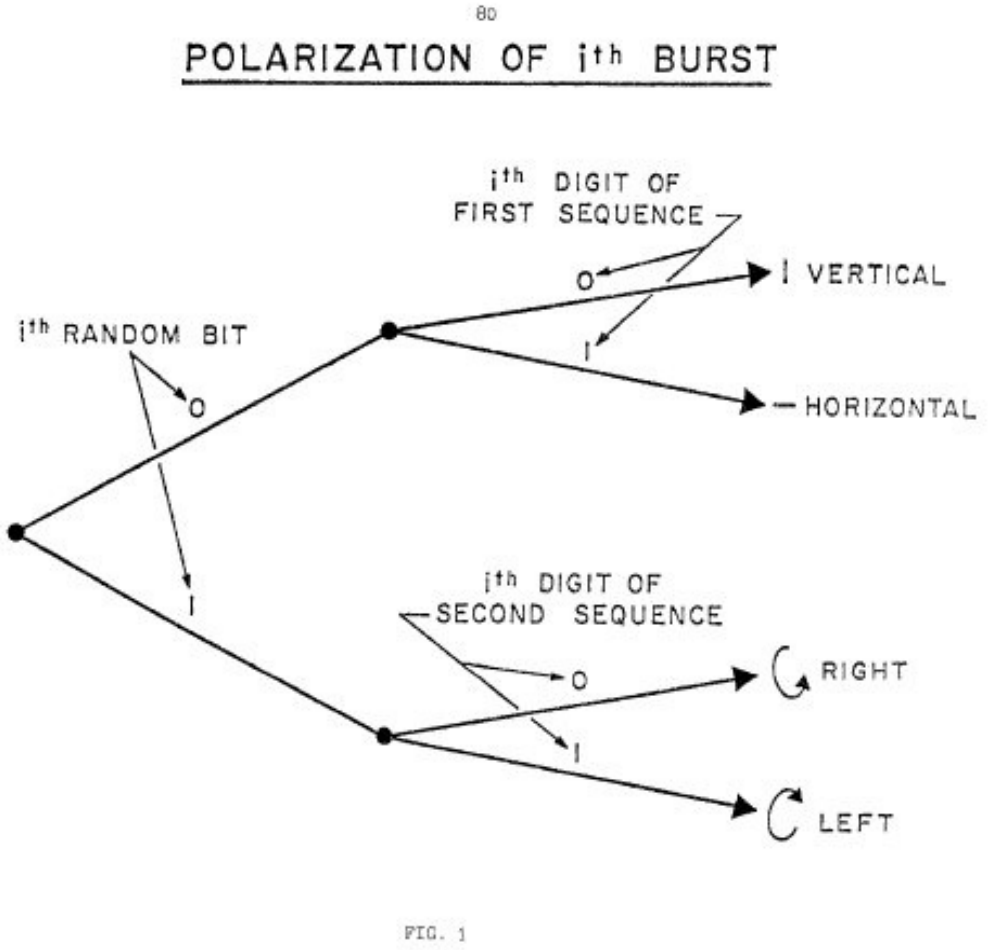


*Figure 2.1. A diagram from Wiesner’s original paper [1] describing the idea of Conjugate Coding using two non-orthogonal bases (of orthogonal polarisations). The idea ultimately led Bennett and Brassard to the BB84 protocol for QKD.*

The second technique described a kind of unforgeable “quantum money” using a set of atomic traps embedded within a monetary token. The use of the conjugate codes here was intended to prevent forgery of the money. A potential forger cannot gain any information about the state of the traps without perturbing the original states, a situation which can later be detected.

As it happens, for various reasons Wiesner’s innovative ideas were rejected at the time, possibly due to the nature of the forum in which he attempted to present his work (IEEE Transactions on Information Theory).

Wiesner’s work was eventually published over a decade later in a special edition of SIGACT news, the publication being triggered by an increasing interest in cryptography and computer science.

Much of the interest in this field was shown by an acquaintance of Wiesner’s named Charles Bennett, then at IBM’s T. J. Watson research centre. Bennett, his main collaborator Gilles Brassard (University of Montreal) and other co-workers were to produce over the next few years a variety of papers on quantum cryptography, coin tossing and other related technologies [9],[10]. In 1984 they presented a protocol for a quantum key exchange using conjugate variables [11] with which, it was claimed, it was possible to exchange a secret key for unbreakable encryption of information for transmission over a public channel. This protocol has since become known as the BB84 protocol (described in chapter 3) and is, perhaps, the basis for the most used QKD protocols today.

Many of the ideas related to quantum cryptography that were proposed during this period were clearly beyond the capability of the available technology to implement and as a result the field was largely ignored by the research community. Eventually, frustrated at the lack of interest in the implications of this technology, Bennett et al decided to build an experimental prototype system and prove the practicality of their ideas.

By the late nineteen eighties, Bennett, Brassard and co-workers had managed to construct an experimental prototype [12], [13] and actually demonstrated a quantum key exchange in the laboratory at IBM [2], [14]. The experiment, now regarded as a classic, used a polarised faint optical pulse scheme to approximate a single photon source and implement the BB84 protocol. Although the transmission distance was limited to 320mm, the experiment not only showed the possibilities for the future but was the first true demonstration of an application of quantum technology. A photograph of the apparatus is shown below in Figure 2.2.

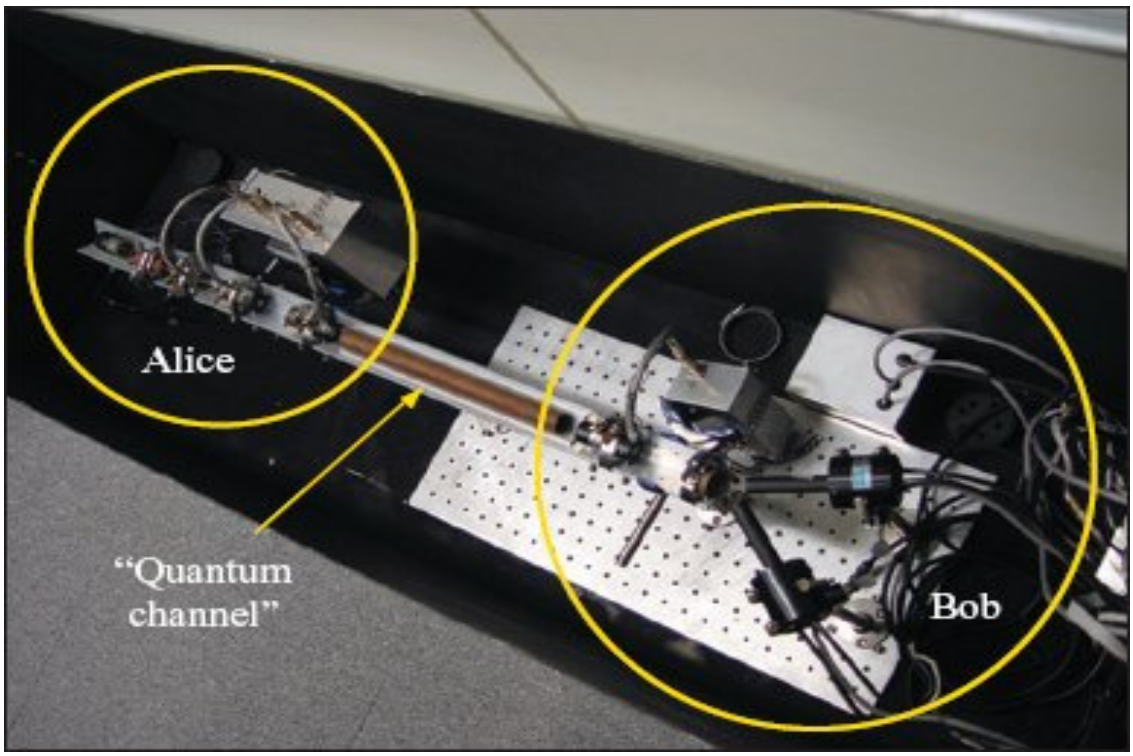


*Figure 2.2. A photograph of the original QKD system built by Bennett et al. The transmission distance (labelled "Quantum channel") was 320mm. (Photograph from reference 7).*

Meanwhile, in Europe, another researcher working at the University of Oxford had proposed a different method for accomplishing the same type of secure key exchange. Artur Ekert, then a PhD. student in the physics department at Merton College outlined a method of quantum cryptography based on quantum entanglement. Whilst his paper [15] was theoretical in nature, it made explicit mention of several current experiments [16], [17] which would provide the basis for a proof of principle. Some while later Ekert, in his own words [18] was fortunate to meet with John Rarity and Paul Tapster, then both at the Defence Research Agency at Malvern, U.K., and propose an experiment to implement his ideas [19].

Rarity and Tapster were already conducting experiments into fourth order interference, nonlocality and other techniques requiring photon correlation [20], [21], [22]. During 1991 the collaboration proved fruitful producing an experimental realisation of Ekert's ideas on public key exchange using quantum correlations. This experiment utilised a parametric down-conversion source of near infrared photons at about 880nm wavelength. These photons were collected and delivered to the distant detector locations via multimode optical fibres over a distance of some 170m. The experimental setup is shown in Figure 2.3.

It is important to note that this experiment used a phase encoding method rather than a polarisation scheme thereby rendering it insensitive to polarisation instabilities in the optical fibre.

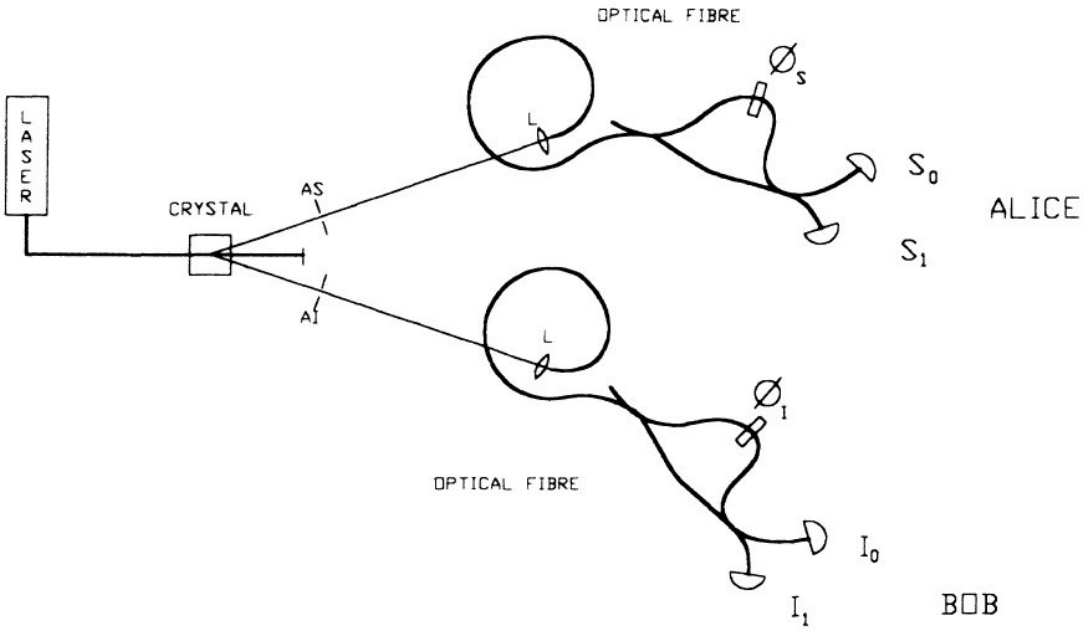


*Figure 2.3. Experimental setup for the Quantum public key distribution system demonstrated by Ekert, Rarity, Tapster and Palma in their 1992 paper [19].*

## 2.4 Childhood, 1992 to 1996

Subsequent to the first demonstrations of QKD, researchers were quick to recognise the potential of this new technology. Although the first implementations were laboratory-based demonstrations of the feasibility of QKD methods, mainly using fibres as the transmission medium, nearly every QKD system reported thereafter demonstrated an innovation in terms of method, or sub-system improvement resulting in increases in transmission distance and key generation rate by orders of magnitude. By 1992, Charles Bennett had proposed a simpler key exchange protocol based on just two non-orthogonal states (now known as B92, [23]) and a phase encoding scheme.

The subsequent year saw the publication of a QKD scheme by a group at the University of Geneva [24]. Nicolas Gisin and co-workers implemented an 800nm weak coherent pulse version of the BB84 protocol utilising polarisation encoding over a 1km fibre transmission line, thus demonstrating that the polarisation scrambling effects of the optical fibre transmission path could be overcome. The experiment is shown below in Figure 2.4.

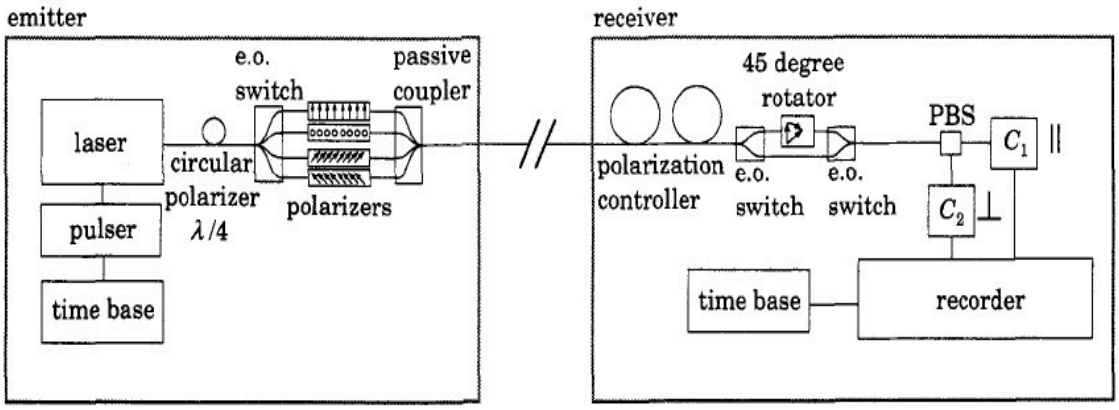


*Figure 2.4. The QKD set up used by Muller, Brueget and Gisin at Geneva in 1993. The system operated a polarisation encoded version of the BB84 protocol at 800nm using a semiconductor laser diode. Key material was exchanged over 1km with a bit rate of ~1kHz and error rate of 0.54%.*

The same year Paul Townsend, John Rarity and Paul Tapster also published work detailing a weak pulse phase encoding system operating over 10km of optical fibre at a wavelength of 1300nm [25], [26]. Based on some of their earlier work on two-photon interference [20], [21], the system was not a complete QKD system, but did demonstrate all the necessary features of a long haul QKD system. Paul Townsend later published work [27] using a virtually identical scheme to exchange keys over the same length of fibre. This system also included error correction and was able to produce keys at a rate of 16kBit/s. The set-up is shown below in Figure 2.5. That same year, 1994 also saw the first publication by an American group at The Johns Hopkins University, Laurel, Maryland. Franson and Ilves demonstrated the essential elements of a key exchange system designed to operate with extremely low error rates in a polarisation scheme using fibre. Although the system used polarisation maintaining fibre over only 10 metres, a bit error rate of 0.5% was reported thereby implying that this system was feasible for exchanging keys over tens of kilometres [28]. The main drawback to this system was reported to be the bandwidth limitation of the polarisation compensation feedback loop and the low final key rate (0.5bit/s). Franson and co-workers continued to develop their system [29], publishing work a year later in which they demonstrated a polarisation based system implementing a BB84 type protocol with a 633nm weak pulse source over 1km of fibre. The system included error correction and privacy amplification based on a Bennett, Brassard and Robert scheme [30].

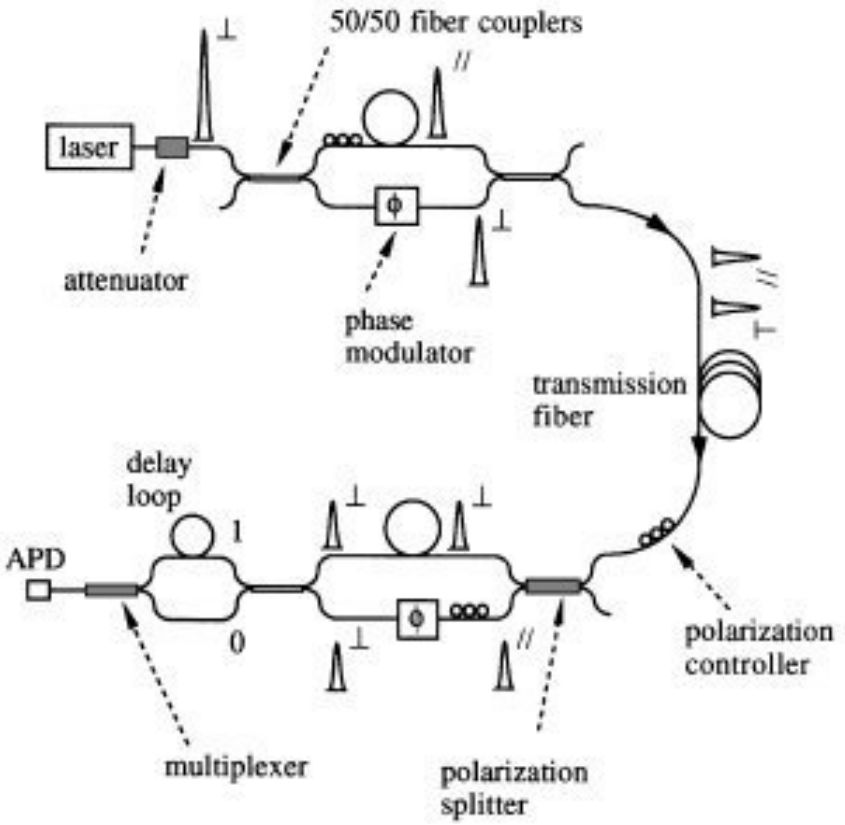


*Figure 2.5. The phase encoding Fibre QKD set-up used by Townsend, Rarity and Tapster in 1994 for a 10km experiment. Although early fibre implementations used polarisation encoding, phase encoding was used almost exclusively after 1995, based on the use of asymmetrical Mach-Zehnder interferometers in both transmitter and receiver. Efficient system operation requires that both interferometers are identical.*

That year also saw publication [31] by Paul Townsend and co-worker, Christophe Marand of an interferometric QKD system running a weak pulse source at 1300nm in standard telecommunications fibre. The system implemented a BB84 type encoding scheme achieving a 4% bit error rate over a 30km range and implemented error correction and privacy amplification.

Another fibre based system reported in 1995 was that of Muller, Zbinden and Gisin working at Geneva [32]. Their polarisation-based implementation of a B92 protocol ran over an underwater installed telecommunications fibre for 23km achieving a bit error rate of 3.4%.

The Geneva group also reported another system running over the same transmission path the subsequent year [33]. Although based on phase, the system utilised a unique two-way transmission path with Faraday mirrors effectively cancelling the effects of fibre birefringence. A novel time multiplexing system also removed the requirement for adjusting the interferometers at either end of the system.

For these reasons the method became known as “plug and play” QKD, reflecting the simplicity of operation of the system. The original “plug and play” experiment is shown below in Figure 2.6

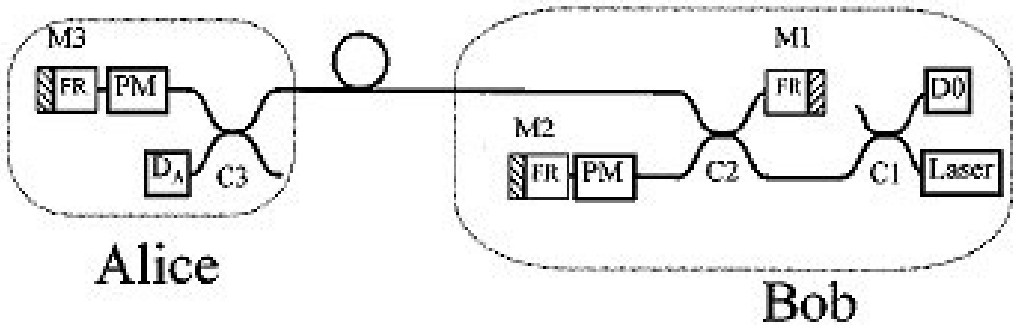


*Figure 2.6. A two-way “Plug and Play” QKD as first implemented by Muller et al (University of Geneva) in 1996, This system, whilst interferometric, removes the requirement for identical interferometers at Alice and Bob.*

*“Bob emits a short pulse, which is split into two. Pulse one travels straight to Alice whilst pulse two is delayed by the M1-M2 delay line. Both pulses are reflected back to Bob at Mirror M3. Meanwhile Alice has measured the intensity of the pulses and attenuated them to single photon intensity. Phase modulators modulate the path length between the pulses. On arrival at Bob, part of pulse 1 is delayed by M1-M2 and thus interferes with the incoming P2. The interference pattern at D0 gives the relative phase settings of Alice and Bob. Use of the Faraday mirrors makes it possible to cancel out birefringence effect due to the transmission medium” [38].*

Another development reported in 1995 by Goldenburg and Vaidman [34] was that of QKD using orthogonal states (up until then QKD had always been performed using non-orthogonal states) The proposed system essentially mimicked a large Mach-Zehnder interferometer, the arms of which formed the (twin) channels.

This year also saw the publication of an important paper concerning entanglement sources [35]. Collaboration between the Universität Innsbruck and the University of Maryland reported a high intensity source of polarisation entangled photons (shown below in Figure 2.7). Previously several sources had been proposed or implemented but suffered from problems of low yield, instability and difficulty of operation.

The new source employed a type II phase matching scheme in a Beta Barium Borate (ß-$BaB_2O_4$ or BBO) crystal and displayed coincidence rates an order of magnitude greater than previously reported experiments.

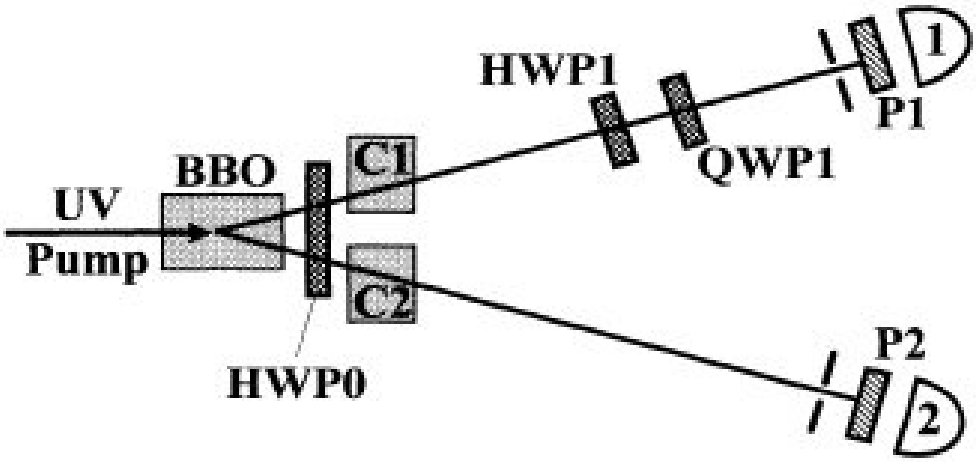


*Figure 2.7. A schematic showing the high brightness entanglement source demonstrated by Kwiat et al in 1995. The source was much simpler than previous sources and yielded higher rates of photons in a polarisation entanglement.*

The first reported free-space system design (since the original IBM experiment) was also presented in 1996 [36]. Franson and Jacobs implemented a free space version of their earlier work in optical fibres. The system used polarisation encoding of weak pulses at 633nm. Whilst the range was limited to ~150m, the system was able to operate over 75m in daylight conditions mainly due to aggressive filtering (both spatial and spectral) at the receiver.

In the few years up to 1996, since its first demonstration, QKD research made much headway (over 30km in fact!). New encoding techniques and protocols coupled with improved technologies such as long wave sources and detectors brought the technology to the threshold of practical system implementation. However, all of these systems were still essentially laboratory prototypes. Both experimentalists and theorists were both still talking about QKD in terms of tens of kilometres and hundreds of bits per second.
Even so, for these modest aspirations there were still numerous engineering and technical problems to be solved. Issues such as power consumption, equipment size and weight, stability (physical, electronic and transmission medium) and reliability all remained to be solved before practical systems could be built. A summary of achievements made during this period is shown below in Table 2.1.

| Year | Achievement |
|---|---|
| 1983 | Wiesner's "Conjugate coding" first published |
| 1984 | Bennett and Brassard propose BB84 protocol |
| 1989 | Bennett, Brassard et al demonstrate first QKD system |
| 1991 | Ekert proposes E91 protocol |
| 1992 | Ekert, Rarity, Tapster and Palma demonstrate QKD based on pair photons |
| 1993 | Correlated photon source<br>1km polarisation based QKD (BB84) |
| 1994 | 10km fibre QKD |
| 1995 | High intensity entanglement source<br>30km fibre QKD |
| 1996 | 23km fibre QKD<br>23km plug and play QKD<br>70m daylight free-space QKD |

*Table 2.1. Summary of main QKD achievements 1983 – 1996.*

## 2.5 QKD reaches puberty, 1997 to 2003

By 1997 several research groups, mainly in the United States and Europe were actively pursuing QKD research for its own sake as well as a useful method of researching Quantum mechanical phenomena. Details of several systems were published during that year including a 200m free space system [37] by the Los Alamos group in the U.S. shown below.

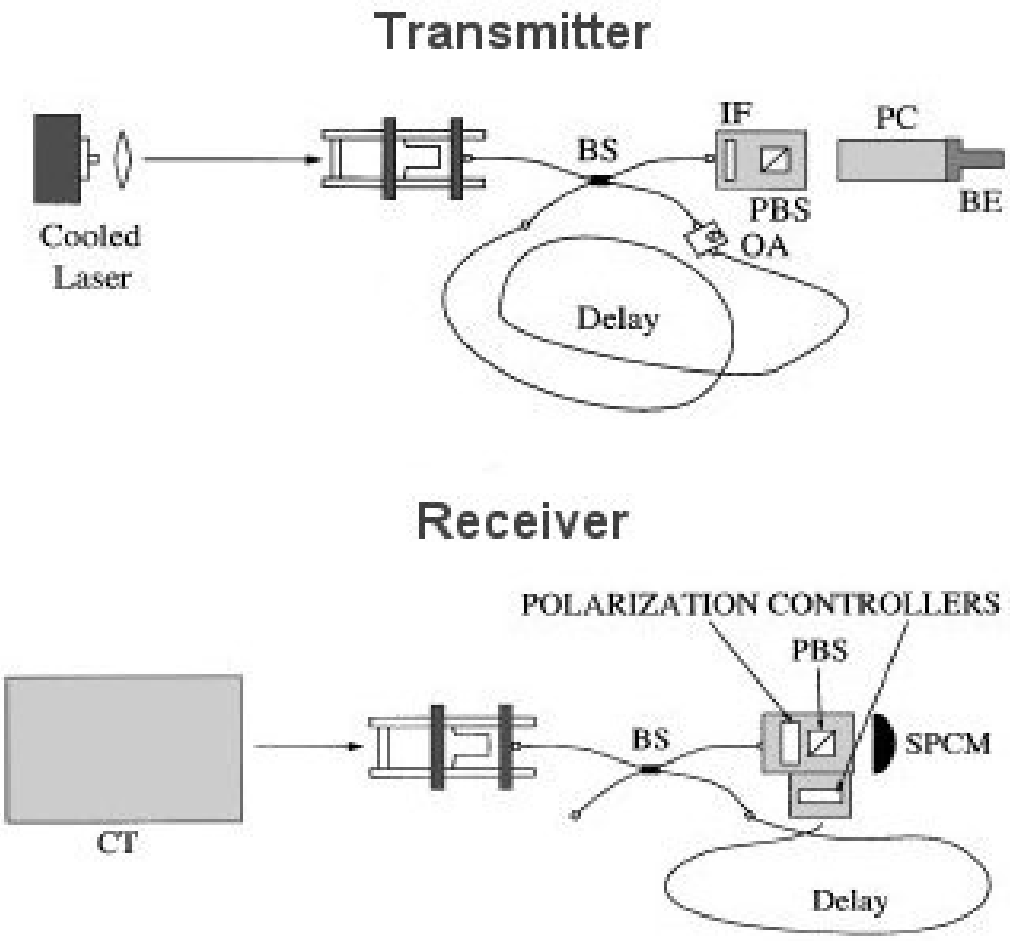


*Figure 2.8. The optical system used by the Los Alamos group in their 1997 indoor free-space experiment. The system, running at 772nm (a convenient atmospheric transmission window) and operating the B92 protocol, exchanged keys with a bit error rate of 6% over the 205m range. A laser is collimated, passed through a beamsplitter (BS), a variable attenuator (OA), interference filter (IF), polarising beamsplitter (PBS) before being modulated by a Pockels cell (PC) and launched into free-space by a beam expander (BE). The receiver collects the radiation in a Cassegrain telescope (CT), focuses it into a fibre, through a beamsplitter (BS), through twin polarisation controllers (for compensation). The radiation is then analysed in a polarising beamsplitter (PBS), with the detection being made with a single photon counting module (SPCM).*

The Geneva group also published further work on their "plug and play" system operating over a 23km fibre link with self-aligning interferometers [38] and Paul Townsend at British Telecom Research Laboratories published a 28km fibre experiment in which both a QKD and communication channel were implemented simultaneously over the same channel [39]. The same year Townsend also published details of a QKD system operating over a passive optical network where the QKD transmitter serviced several receivers via a passive optical splitter [40].

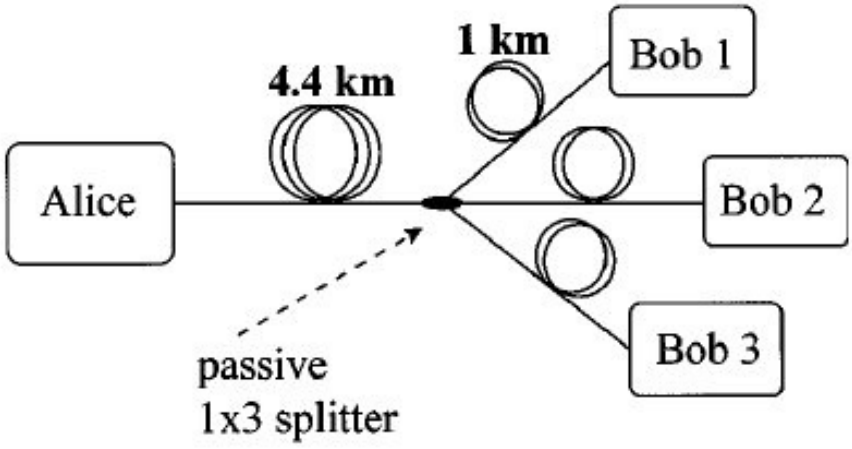


*Figure 2.9. The experimental set-up used by Paul Townsend in 1997 to demonstrate QKD over Passive optical networks (PONs). The experiment successfully exchanged keys over several kilometres in practical scenarios [40].*

The following year, 1998, was a quiet one. Several groups published work on quantum entanglement. A group at the Universität Innsbruck conducted an experimental violation of Bell's inequality [41] under strictly enforced locality conditions [42]. Whilst not strictly QKD, such experiments were important from the point of view of further validating concepts central to Quantum Mechanics and some of its properties, particularly those of nonlocality. These ideas were and still are central to the working of entangled state QKD[1].

Richard Hughes also published further work with the LANL free space system [43] and the year closed with the start of the first European Community funded quantum cryptographic collaboration [44] featuring research groups from the U.K. (DERA, U. Oxford), Italy (Elsag-Bailey Spa, Genoa), Germany (LMU Munich), Austria (U. Vienna) and Switzerland (U. Geneva).

[1] Entangled state implementations of QKD invariably involve a measurement of a violation of Bell's inequality as a proof of their validity.

The project, named EQCSPOT (European Quantum Cryptography and Single Photon Optical Technologies), featured both industrial and academic partners and was designed to raise the technology maturity level of QKD and its various subsystems (including software and detectors for long wavelength operation). Co-ordinated by John Rarity at DERA in Malvern, U.K. the program included some of the major researchers in the field and was notable in that a complete work area was devoted to software development including a graphical user interface with the necessary applications interface to the QKD hardware layer. A further work area was also devoted to the study of the feasibility of ground to satellite links for QKD, thus recognising a requirement for global reach of QKD.

By 1999 the area of QKD research was in full swing with several active research groups publishing a wide range of research. A Swedish group published activity [45] on an interferometric plug and play QKD scheme which utilised InGaAs SPADs running at 1550nm, the first such system to do so. This research was particularly relevant as for the first time QKD was demonstrated to be compatible with existing telecommunications network infrastructure. The same year also saw publication of three entanglement-based systems [46], [47], [48] by groups in Germany/Austria, Geneva and the U.S. The systems implemented Ekert's B91 [15], BB84 [11] and a novel energy-time protocol respectively. All three experiments demonstrated the feasibility of long distance operation of entanglement-based systems and featured enhanced security (through the means of entangled pair sources), whilst two of the systems also implemented continuous monitoring for eavesdroppers.

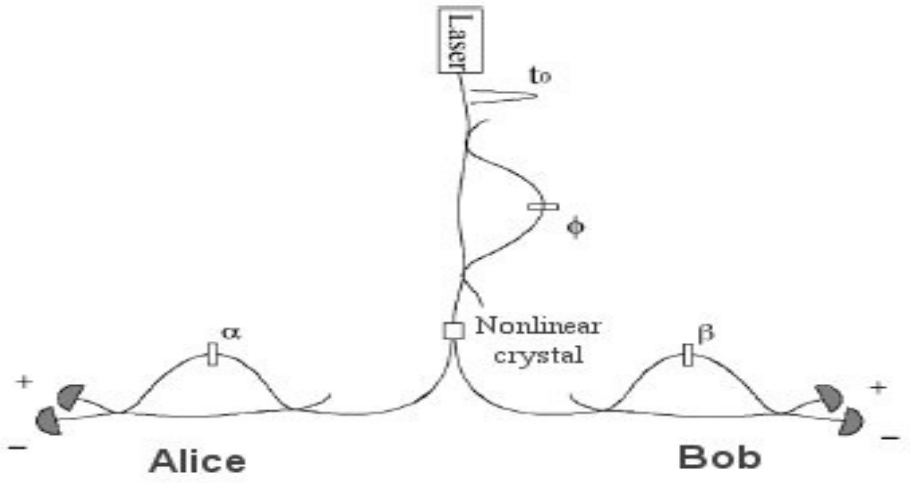


*Figure 2.10. The entanglement based experiment by Tittel et al at the University of Geneva was the first such setup to use 1310nm entangled pairs making the system compatible with telecommunications fibres. Both Alice and Bob interferometers were subject to instabilities.*

The Geneva experiment was also the first to implement long wave operation in a photon-pair system at a wavelength compatible with ordinary telecommunications fibres (1310nm). Detection was achieved with aggressively cooled (77K) Germanium avalanche photodiodes.

The energetic Los Alamos team saw in the new millennium with a daylight key exchange over 1.6km featuring the B92 protocol and bright pulse timekeeping [49], a 48km fibre point to point key exchange featuring interferometric versions of both BB84 and B92 (with bright pulse timing) [50] and a ground to satellite feasibility study based on results from their free-space experiments [51].

Another free-space system demonstrated that year was a 1.2km BB84 implementation by the Rarity team at the Defence Evaluation and Research Agency (DERA) at Malvern, U.K. The system (shown below in Figure 2.11), based on Acousto-optic beam switching, featured automatic key sifting, error correction and privacy amplification and a novel timekeeping system based on a software phase-locked loop, thereby negating the requirement for a bright timing pulse [52].

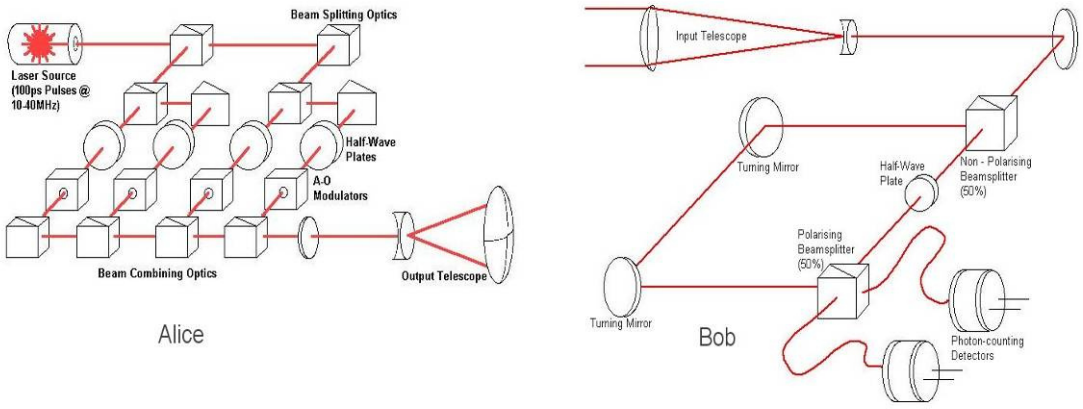


*Figure 2.11. The free-space set up used by Rarity and colleagues in their 1.2km, BB84 key exchange experiment in 2000. The system operated with a multiplexed single source, switched by A-O modulators. The receiver made use of a delay line to time multiplex the SPAD modules. Each terminal was approximately 1m$^2$.*

The year 2000 also saw publication of two entangled state QKD systems. A collaborative team from the University of Vienna and from Ludwig Maximillians Universität in Munich implemented a polarisation entanglement based system capable of realising both the Ekert 91 and BB84 type scheme over 360m, achieving an 850bits/sec final key rate with a 2.5% bit error rate [46]. The system also featured Rubidium timing standards and detector basis selection by random number generator.

The experiment was also notable as the first full and practical implementation of entangled state quantum cryptography. The second system, reported by the GAP Optique team at the University of Geneva implemented an energy-time entangled system over 8.5km of optical fibre [53].

The system achieved key rates of 134Hz at an error rate of 8.6%. Notably, this system used a non-degenerately tuned source producing photon pairs with wavelengths of 810nm and 1550nm (This type of source is invariably a variety of parametric down-conversion source wherein a non-linear optical crystal is pumped by a laser. The pump photon is "split" into a signal and idler photon, the sum of whose energies is equal to that of the pump photon. The crystal is usually cut such that its orientation produces signal and idler photons of identical wavelength, which is known as degenerate tuning. If the crystal is cut such that differing wavelengths are produced, then it is said to be non-degenerately tuned). This innovation enabled use of efficient Silicon avalanche detectors at the local receiver (Alice) whilst allowing the exploitation of the excellent transmission properties of optical fibres [54] at 1550nm for the remote receiver (Bob). The system (shown below in Figure 2.12) also used an optical classical channel operating over fibre at 1550nm.

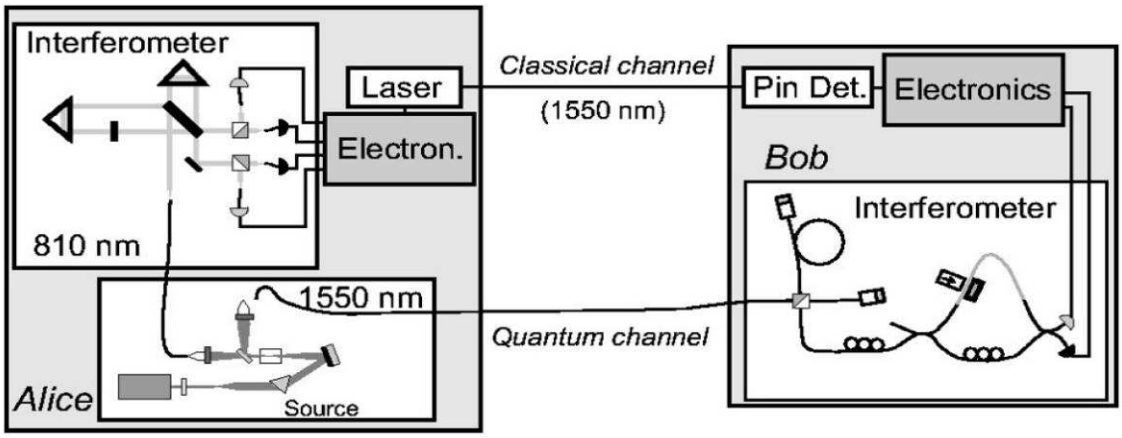


*Figure 2.12. The asymmetrical entanglement based QKD system used by GAP. The entangled photon pair are non-degenerate, i.e. they posses different wavelengths. One photon is detected locally with high efficiency silicon SPADs whilst the other is sent, at low loss, over telecommunications fibre to the remote detector. Classical communications is provided by an optical channel.*

Both of the entangled state systems were part funded by the second European community funded project to fund quantum technologies [55]. The project, named IST – QuComm (Long Distance Photonic Quantum Communication) featured teams from Sweden, Germany, France, Switzerland, Austria, United Kingdom, as well as the Los Alamos team from the U.S.

Early in 2001, the Rarity team at Malvern, U.K. published more of their work on free-space QKD [56]. The system, a weak coherent pulse implementation using the BB84 protocol, was shown to exchange keys over 1.9km with a transmission loss of >20dB. This result was important in that it demonstrated the ability of QKD systems to withstand the channel losses associated with performing QKD to satellites.

The rest of the year was quiet except for an interesting paper [57] by a collaboration between the University of Geneva and the Université de Nice-Sophia Antipolis, Nice. Tanzilli and co-workers demonstrated a waveguide based entangled pair source fabricated from periodically poled Lithium Niobate substrate. The device produced a high intensity beam of 1314nm photons and, significantly, was pumped by a semiconductor laser at 657nm.

If 2001 was a quiet year for QKD research 2002 was to prove to be highly productive with over 7 papers published on QKD. A 10km fibre autocompensating system was presented by Bethune and Risk [58], both at the IBM laboratories at Almaden, California. The system operated over standard telecommunications fibre at 1.3μm wavelength with timing information multiplexed over the same path at 1.5μm and used a standard LAN connection for the key reconciliation.

Another 10km system reported that year, this time by Richard Hughes and his team at Los Alamos National Laboratory in the U.S., was a 772nm wavelength free-space system implementing the BB84 protocol [59]. This sophisticated system featured narrowband filtering at the receiver, allowing operation during daylight, whilst timing synchronisation was provided by a 1.5μm optical pulse. Key reconciliation was performed using a wireless Ethernet public channel.

A night-time key exchange system was also reported this year by two teams (DERA at Malvern U.K. & LMU Munich, Germany) of the EQCSPOT collaboration [60]. The system, shown in Figure 2.13 below, featuring miniaturised transmitter and receiver modules, was shown to transmit cryptographic keys over 600m in metropolitan Munich and a 23km range in the Bavarian Alps using an optical public channel and a G.S.M mobile telephone link respectively for key reconciliation. Synchronisation was provided by a software phase-locked loop deriving its timing information from the receiver detections rather than a bright pulse.

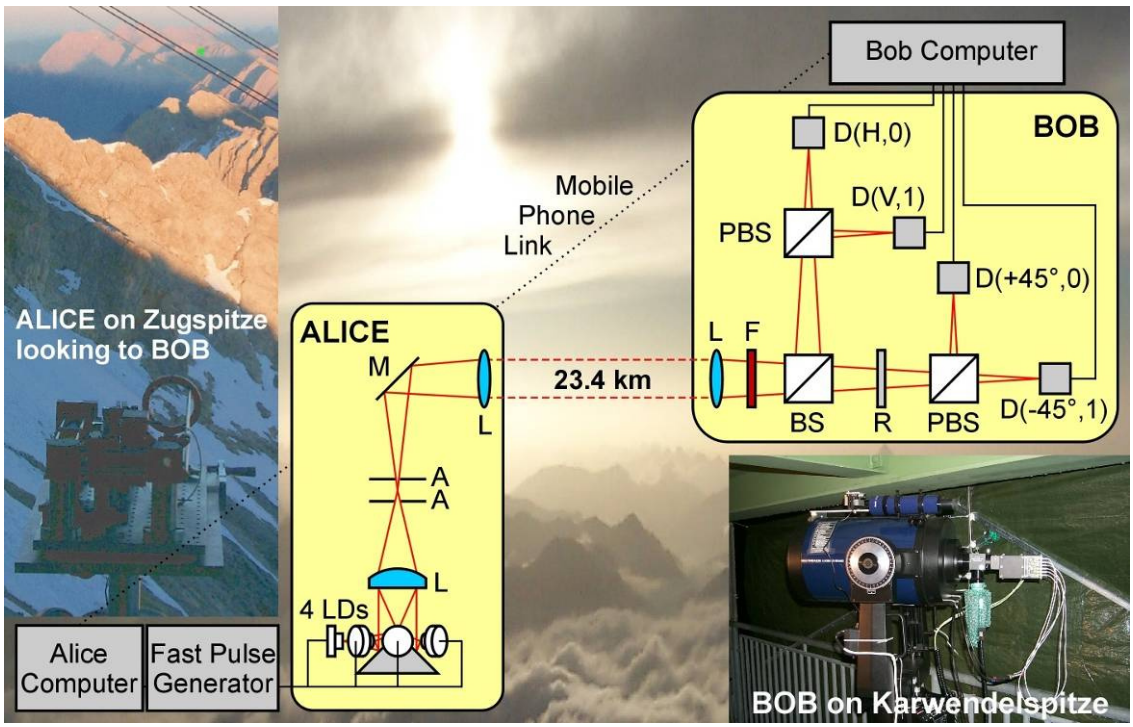


*Figure 2.13. A diagram showing the 23.4km free-space experiment in the Bavarian Alps by members of the EQCSPOT collaboration in 2002. The Alice and Bob terminals were situated in facilities (cable car stations) at the summit of two of the highest mountains in Germany.*

Another EQCSPOT team also reported a QKD system, this time operating over 67km of fibre at 1.5μm wavelength [61]. The GAP Optique team at the University of Geneva showed their system, a “plug and play” phase-based system packaged into two industry standard 19” boxes, operating in real conditions including installed aerial cables. Interestingly, two of the authors were shown as having affiliation with a commercial company called ID Quantique, a company founded in 2001 by the Geneva team in order to commercialise this technology, one of the first commercial companies to do so [62].

The same year also saw publication of theoretical papers on new QKD protocols featuring continuous variables by Phillipe Grangier and co-worker at the Laboratoire Charles Fabry de l’Institut d’Optique, in Paris [63], and also further work on entanglement generation in waveguides by a team at the University of Boston [64]. Lastly, based on recent achievements by several teams, Rarity et al published [65] a feasibility study detailing several methods of achieving satellite key exchanges between ground stations and low earth orbit.

The year of 2003 continued the strong level of activity for QKD research. A small ESA funded study called QSPACE (Quantum communications in Space) reported findings and recommendations by two groups for space-based experiments into quantum information technologies [66].

The two groups were the usual suspects from the European QKD community (Rarity, Weinfurter, Gisin, Zeilinger and co-workers). An American collaboration also reported on the performance of QKD through transparent optical switches [67]. The team implemented a B92 protocol through several types of optical switch and successfully exchanged keys through a reconfigurable transmission path, thus taking an important step toward network-based QKD.

Fibre systems were also reported by two Japanese teams. Kosako (NEC) and co-workers [68] reported a 100km interference experiment utilising a "plug and play" system operating at 1.5μm with a novel balanced detector, whilst a team at Mitsubishi Electric Corporation claimed a world distance record of an 87km key exchange over fibre using their compact, integrated QKD system (actually achieved during 2002) [69]. A summary of the main advances in QKD made during this period may be seen below in Table 2.2.

| Year | Achievement |
|---|---|
| 1997 | Violation of Bells inequality over 35m<br>28km QKD in fibre<br>23km "plug and play" QKD in fibre<br>205m free-space indoor QKD (B92) |
| 1998 | Quantum correlations over 10km of fibre<br>50km point to point phase encoded in fibre<br>EQCSPOT collaboration starts<br>1km night-time free-space QKD (B92) |
| 1999 | 360m polarisation entangled QKD (BB84)<br>40km "plug and play" QKD in fibre at 1550nm<br>Ultra-bright polarisation entanglement source |
| 2000 | 8.5km entangled state QKD<br>48km point to point fibre demonstration<br>23km "plug and play" QKD in fibre<br>1.2km night-time (BB84)<br>free-space QKD 1.6km<br>daylight free-space QKD(B92) |
| 2001 | Waveguide pair sources<br>2km free-space |
| 2002 | 67km "plug and play" QKD in fibre<br>10km daylight free-space<br>24km nightime free-space QKD (BB84)<br>Continuous variable QKD<br>Ground to LEO QKD feasibility. ESA funded<br>QSPACE program starts |
| 2003 | QKD in space feasibility<br>QKD through reconfigurable optical switches |

*Table 2.2. Summary of outstanding QKD achievements from 1997 to 2003.*

## 2.6 QKD comes of Age, 2004 to 2009

By 2004, research into Quantum Key Distribution had morphed into something much larger and with a huge potential. The original researchers of QKD had, perhaps, pursued this application as a vehicle for researching other interesting phenomena such as Quantum Entanglement, Quantum logic and Quantum Communications. Ultimately though, these research areas were to unify to become the research field of Quantum Information Technology.

As mentioned earlier, many researchers were all too aware that their experimental systems lacked practical abilities for real world applications, however, several Universities set up "spin out" companies to attempt to ruggedise the technologies. During this period several private venture companies were also set up with a view to commercialising QKD systems, moreover, global names such as Toshiba [71], NEC [72], and Mitsubishi [69] were appearing frequently as affiliations in the peer reviewed literature. However, despite almost continuous funding by the E.C. and the U.S. Government for over a decade, there appeared to be a worldwide lack of understanding on the part of governments, and, on the face of it, commercial customers. The only obvious exception to this, unsurprisingly, was the Government of Japan who were already funding a national strategy through several government departments. The strategy was implemented over 5 year phases with phase 1 commencing in 2001 [121].

The period started briskly with an Austro-German collaboration implemented an entangled state QKD system running over 1.5km of fibre installed in the sewers under the city of Vienna (see Figure 2.14. below)

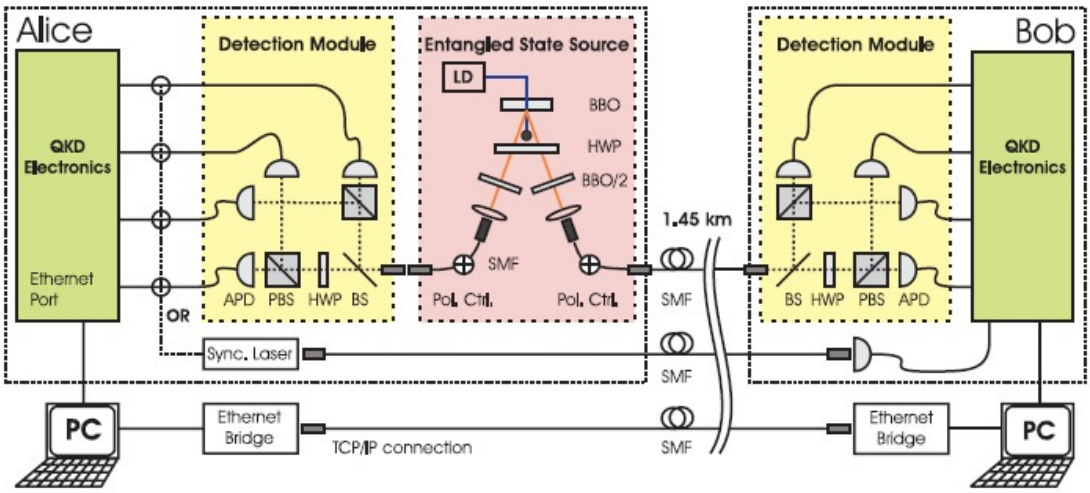


*Figure 2.14. The entanglement-based fibre-through-the-city-sewers experiment by an Austro-German collaboration in 2004. The generated keys were immediately made available and were used to secure a financial transaction.*

The resulting secure keys from this experiment were handed over and used to secure a financial transaction between Vienna city hall and Bank-Austria Creditanstält [70]. This paper also lists three companies as actively selling commercial QKD systems, idQuantique, MagiQ and N.E.C. In another fibre experiment, a team at Toshiba Research Europe reporting a 122km key exchange at 1.5μm wavelength in telecommunications fibre [71]. The system, based on a weak pulse, phase implementation of the BB84 protocol was able to produce raw sifted key material at ~10bits/s with a bit error rate of ~9%.

A free-space experiment was also reported by a team at NIST in the U.S. [73]. J. C. Bienfang and co-workers were able to demonstrate a gigahertz clocked QKD system over a free-space range of ~730m with sifted key rates of up to 1Mbps, several orders of magnitude greater than previously reported systems, rendering QKD compatible with the requirements of modern information technology (for example video streaming). Another gigahertz class system was also demonstrated [74] by Gerald Buller and his team at Heriot-Watt University in Edinburgh and Paul Townsend at the University College Cork, Eire. The system implemented a polarisation version of the B92 protocol at 850nm over 10km of fibre achieving key rates of 7kBits/s at 2.1% bit error rate.

The year also saw the start of a large European community funded project known as SECOQC (Development of a Global Network for Secure Communication based on Quantum Cryptography) [75]. The project, lasting four years and funded to the amount of 11.4 million Euros, consisted of 41 partners from 12 countries consisting of three SMEs, 25 Universities, five national research centres, and eight private enterprises.

By 2005 QKD systems were clearly becoming more sophisticated but still tended to be point to point links operating independently. A team from BBN technology in Cambridge, Massachusetts, published work on their “Quantum Network” [76], shown below, which had, in fact, been operational in limited form since 2002. The network consisted of six nodes operating over telecommunications fibre around the Boston Metropolitan area, with a further four planned. Intended as a test bed for QKD, the network included innovations such as optical switching for several of the nodes and a suite of network management protocols common to all of the (differing) QKD systems.

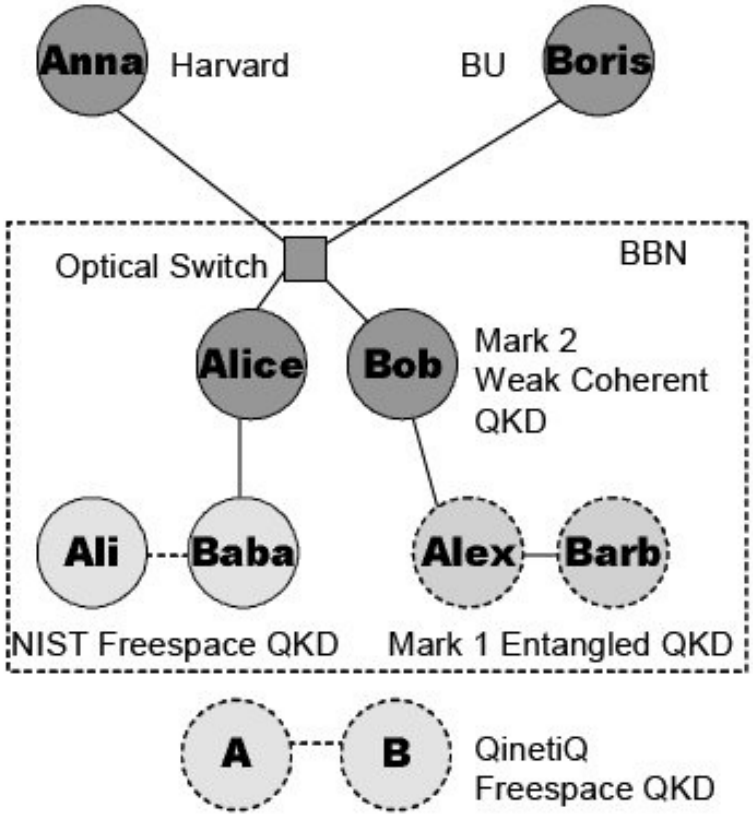


*Figure 2.15. Network topology of the DARPA Quantum Network [66] showing a variety of QKD technologies linked together. The network included several QKD technologies with a free-space node provided by QinetiQ from the U.K.*

Several fibre based systems were also reported this year. Zhou et al at the University of Toronto performed QKD over a 15km fibre path using a commercial plug and play system manufactured by idQuantique [77]. Whilst the transmission length and bit rate of the experiment were pretty ordinary by 2005 standards, the experiment introduced Decoy State QKD for the first time building on work by Hwang [78] and previous work by the authors [79], [80] and Wang [81], [82]. This new adaptation of BB84 was of considerable importance due to the ability of the decoy state protocol to increase key rates and security without resorting to exotic technology. Until this time most weak coherent pulse QKD systems had, somewhat arbitrarily, chosen a mean photon number for pulse transmission of 0.1photons per bit (This does not strictly satisfy unconditional security requirements demanded by, for instance, [82]. The 0.1phots/bit figure arises from the Poissonian emission statistics of lasers and is further discussed in chapter 3).

Another fibre system reported was that of Andrew Shields and his team at Toshiba in Cambridge.

The reported system [83] essentially the same as that reported previously in [70] was run continuously over 20km of installed telecommunications fibre with active compensation.

Another experiment demonstrating the practicality of modern systems was reported by a commercial collaboration between MagiQ and MCI scientists [84]. This experiment successfully employed a commercially available QKD system and deployed it over a 50km WDM fibre link using industry standard ITU grid C-band wavelengths [85].

In another fibre experiment [86], a collaboration between Heriot-Watt University, Politecnico di Milano and University College Cork (Buller, Cova, and Townsend) ran a short wavelength (850nm) fibre system detailed in [74] at up to 2GHz. Improved detectors allowed the system to function with improved bit error rates (7% over 6.5km) with the potential for increased key rates and transmission distance.

By contrast the entangled state QKD scene was quiet with two free space experiments reported. Resch et al at the University of Vienna (the team also included members of the LMU team at Munich and the National University of Singapore) managed a night time entanglement distribution over a 7.8km free-space range using polarisation correlations [87]. Meanwhile Peng et al (University of Science and Technology of China, Hefei) conducted a similar experiment [88] over a range of 13km, both experiments exceeding transmission through the one equivalent air mass necessary to reach low earth orbit.

By 2006 the field of QKD was becoming ever popular with research groups from Europe, USA, China and Japan dominating the field. Numerous research papers on all aspects of QKD were being published. Continuing the theme of improving on existing systems and sub-systems many groups were publishing updates and improvements on previously work. The NIST group (collaborating with the University of Maryland) published work on their high speed polarisation over fibre system [89] achieving sifted key rates of 2Mbits/s with an error rate of ~3%. The team also published intentions to overhaul the free-space system described in [70] to achieve secret key rates of 10Mbits/s [90]. The NIST team also demonstrated [91] a novel fibre QKD system using ultra low noise Superconducting Transition Edge Sensors (TES) detectors in a collaboration with the QKD group at LANL. (TES: Very thin films of superconducting material with a sharp resistive transition which can be used as extremely sensitive calorimeters. See [122]),

The combined team achieved several new transmission records including an absolute QKD transmission distance record of 184.6km using a mean photon number, $\mu$, of 0.5photons/bit.

Another long distance experiment was that of Takesue et al (collaboration between NTT Corporation, Japan, and Stanford University, U.S.). Building on previous successful and world leading experiments with a relatively new protocol (Differential phase shift QKD [92], & [93]). The system used novel up-conversion detectors and successfully generated useful key rates over 100km of fibre [94]. Upconversion detectors are a relatively new method of single-photon detector which makes use of sum-frequency generation in non-linear crystals to produce a frequency shift in the optical signal beam. The method allows, for instance, detection of 1.5μm photons using highly efficient and low jitter silicon-based single photon counting detectors. See for instance [123], [124], [125] & [126]. Importantly the system was designed to produce key material secure against all allowed quantum mechanical attacks.

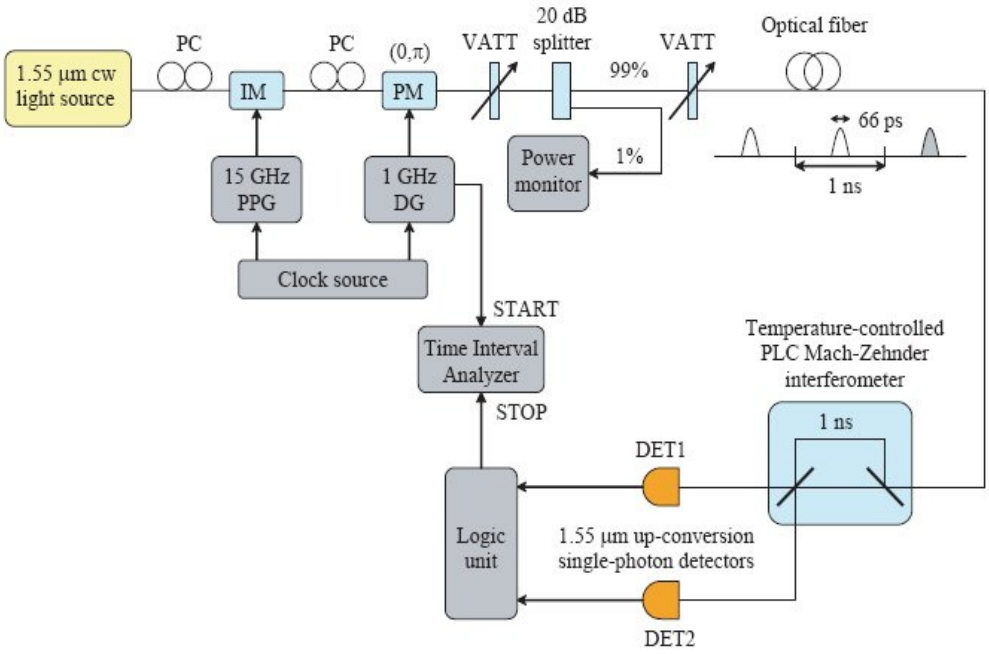


*Figure 2.16. The experimental setup used by Diamanti et al in their 100km, 1GHz clocked DPS QKD system. The system used low jitter upconversion detectors, allowing greater bit rates and longer distance operation.*

Other fibre QKD implementations tested this year included a 3.3GHz clocked system from the Heriot-Watt group in collaboration with Paul Townsend at University College, Cork [95], unusually the system operated over standard telecommunications fibre at a short wavelength of 850nm (thanks to some novel beam launching techniques, thereby limiting transmission distances due to attenuation, but also allowing the use of efficient Silicon SPADs (Single Photon Avalanche Diodes). The same system was also applied to demonstrating QKD over passive optical networks [96].

Lastly for this year an interesting publication by the first Israeli team proposed a free-space QKD system [97] using a space-division multiplexing idea wherein the secret bit rates could be increased by using multiple transmitter and receiver channels. Dubbed MIMO (multiple input multiple output) QKD, the modelling of the system predicted that atmospheric turbulence would give rise to crosstalk induced errors. The team proposed the use of wavelength division multiplexing to overcome this problem.

It appeared that 2007 was to be a good year for QKD research with a whole raft of publications on entangled state sources, entanglement-based QKD experiments and several long haul, high bit rate QKD systems.

A remarkable pair of experiments reported this year were twin long haul experiments in free space. Sponsored by the European space agency (ESA) and part funded by SECOQC a team composed of multiple nationalities managed a key exchange over 144km [99] between the Canary islands of La Palma and Tenerife. These locations are host to the Instituto de Astrofisica de Canarias (IAC) which administers the twin observatories of O. Teide and O. Roque de Los Muchachos, home to the European Northern Observatory (ENO). Only one pair of telescopes can see each other from each location, the Nordic Optical Telescope (N.O.T.) on La Palma and the ESA owned Optical Ground Station (O.G.S.) on Tenerife. One experiment used degenerate down-converted photon pairs at around 800nm with a closed loop tracking system to compensate for atmospheric distortion whilst the second used the same apparatus but replaced the emitter with a compact decoy state transmitter. The experiments exceeded previous free-space QKD transmission distances by an order of magnitude and demonstrated further the feasibility of ground to satellite, and therefore global, QKD. A diagram of the optical set up of the decoy state experiment is shown below in Figure 2.17.

In another experiment, the first use of entanglement in a Differential Phase shift implementation of QKD was reported [98]. Honjo, Takesue (NTT) and Inoue (JST) used a fibre source of entangled photons in a laboratory-based experiment. This experiment was also notable in that it was the first to actually exchange key material with degenerate photons at 1.5μm.

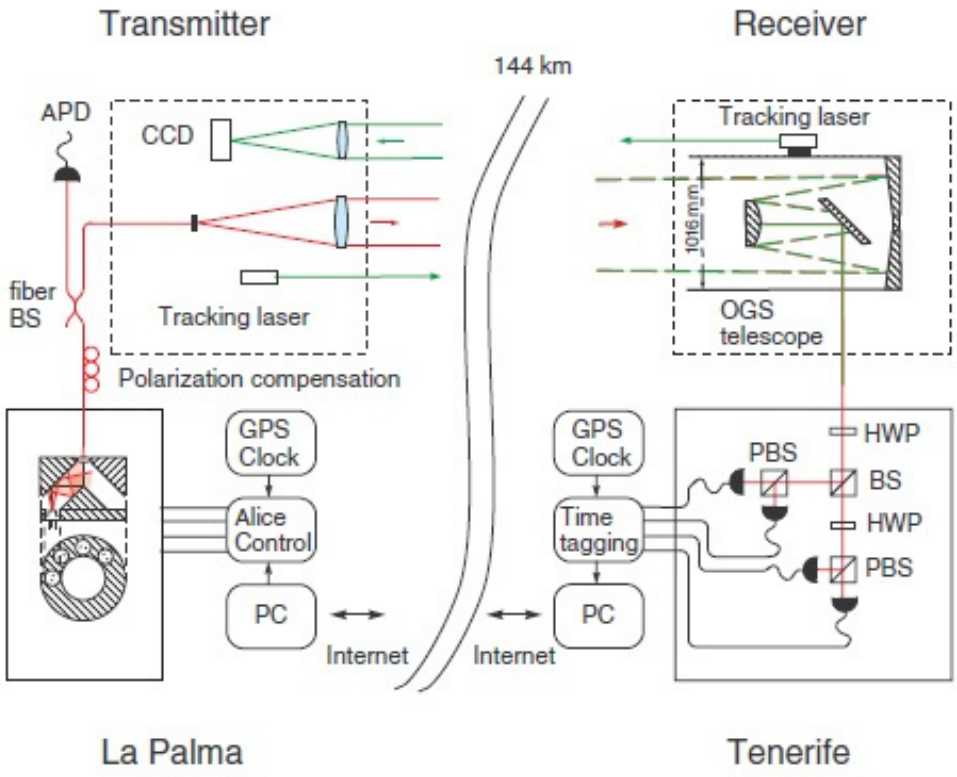


*Figure 2.17. The Decoy state experimental system used in an ambitious experiment over a 144km range at the Canary Islands. The experiment used a compact transmitter coupled to a small output telescope on La Palma, whilst the receiver was integrated into an astronomical telescope located on Tenerife. The same range was also used for an entanglement-based experiment.*

Several other ground breaking fibre-based experiments were also reported this year. Namekata and a team including Honjo and Takesue from NTT corporation reported a DPSK-QKD experiment [101] in which they exchanged keys over 15km of fibre, achieving a sifted key rate of 1.5Mbits/s (0.33Mbits/s secure key) at a bit error rate of ~2.3%. Bit rates of 100kbits/s were still achievable after 40km. It should be noted, however that the transmission medium was dispersion-shifted fibre and not ordinary telecommunications fibre. This experiment was also noteworthy due to the use of sinusoidally gated InGaAs SPADs running at 500MHz.

The team at NTT also reported, in collaboration with NIST and Stanford University, a 200km key exchange with a 42dB loss tolerance [102]. The experiment was made possible by the first reported use of NbN superconducting nanowire detectors and an exceptionally high clock rate of 10GHz. These detectors exhibit low quantum efficiency but this is offset by an exceptionally low dark count, a very good timing jitter (allowing high speed operation), no afterpulsing and a broadband response. The downside is that operation requires cryogenic temperatures.

Other fibre-based implementations of QKD were reported this year. The Toshiba group reported continuous operation for 60 hours over 20km with a decoy state system achieving a record 10kbits/s key generation rate [103]. Meanwhile the Heriot-Watt/University College Cork group published work [104] in which 3GHz clock rate QKD was implemented over two types of passive optical network (PON) of the type currently being installed over last mile type networks.

In addition to QKD systems it appeared that maturity in practical entanglement sources was growing. The source of choice for QKD and other quantum mechanical experiments was usually constructed by exploiting parametric fluorescence in periodically-poled non-linear crystals. The problem with existing entanglement sources, which invariably used bulk crystals, was that they tended to be large and ungainly (not to mention the large-frame lasers and their associated cooling plant employed as pump sources for these rather low yield devices). These new sources possessed the necessary properties to produce compact, stable, reliable and intense sources of entanglement that could be fibre coupled and pumped by semiconductor lasers. This type of source had been in development for some years and was used in the original 1991 experiment by Ekert et al. The intervening years have seen a process of development. (See [105] - [113]) with the resulting sources becoming compact, robust and high yield with excellent entanglement characteristics. Several types of non-linear crystal were used such as Potassium Titanyl Phosphate (KTP) in the case of [98] and [106] and Lithium Niobate (LiNbO3) in the case of [107], [108] and [109]. Other improvements included the use of waveguides, fibres and semiconductor lasers as pump sources.

By 2008 QKD advances were being reported almost continuously and practical systems were beginning to produce really useful key rates over inter-city distances. A collaborative team at NEC and including NIST at Boulder implemented a phase-based BB84 system over 97km of installed telecommunications fibre [114]. The system used Niobium Nitride (NbN) superconducting detectors and running at a clock speed of 625MHz achieved a record key rate of 2.4kbps at an error rate of 2.9%. A novel method of system synchronisation was also tested in this experiment, whereby the system clock was transmitted in an adjacent WDM channel. This record was not to stand for long however. Andrew Shields and his team at Toshiba reported a phase-based decoy state system running at a 1GHz clock speed [115]. This system employed novel InGaAs SPAD detectors gated at 1.036GHz (pictured below).

As a result, the detectors displayed an ultra-short dead-time (an important figure of merit for single photon avalanche detectors further expanded upon in chapter 3) between detections and allowed extremely high detection rates. In addition a novel self differencing circuit was coupled to the output for effective noise cancellation. This combination allowed the system to achieve an outstanding key rate of 1.02Mbits/s over 20km of fibre.

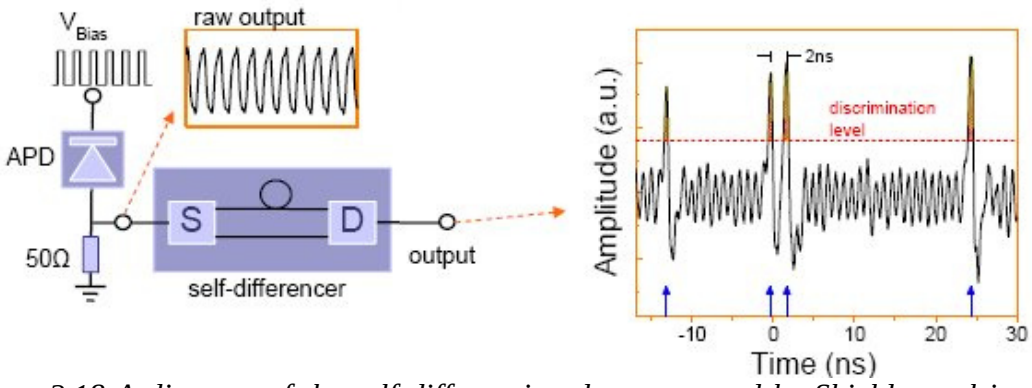


*Figure 2.18 A diagram of the self differencing detectors used by Shields et al in their 2008 experiment. Use of the self-differencing circuit gives excellent noise cancellation and allows for smaller avalanches to be detected. Smaller avalanches with less charge moving through the SPAD device leads to lower afterpulsing. This in turn allows much faster detector gating.*

Not only were long haul fibre transmission experiments being performed with weak pulse setups, other teams were pursuing entanglement-based research. A collaboration between NTT Corporation, NIST, NICT and Stanford University succeeded in transmitting photons from a centrally located entanglement source to two receivers over separate 50km fibre paths, resulting in a 100km key exchange, the longest at the time [116]. The system included planar lightwave circuit (PLC) interferometers and Niobium Nitride (NbN) superconducting nanowire detectors and achieved bit rates of 0.57bps at an error rate of 6.9%.

The first daylight free-space entanglement experiment was also reported this year by a team at the National University of Singapore [117]. Using a fairly typical entanglement system, the team implemented strong spatial, spectral and temporal filtering to remove the strong solar background and continuously exchanged keys over 350m at a rate of 358bps over several days.

In another free-space experiment, this time at night, a team from the University of Waterloo, Canada implemented the first real time QKD link between two locations with no direct line of site, the source being placed in a potentially hostile location [118]

(It is a property of entanglement-based QKD systems that the source of photons can be placed in a location that is potentially untrustworthy). The system was shown to exchange keys over a 1.525km link at a secure key rate of 85bits/s and an error rate of 4.92%.

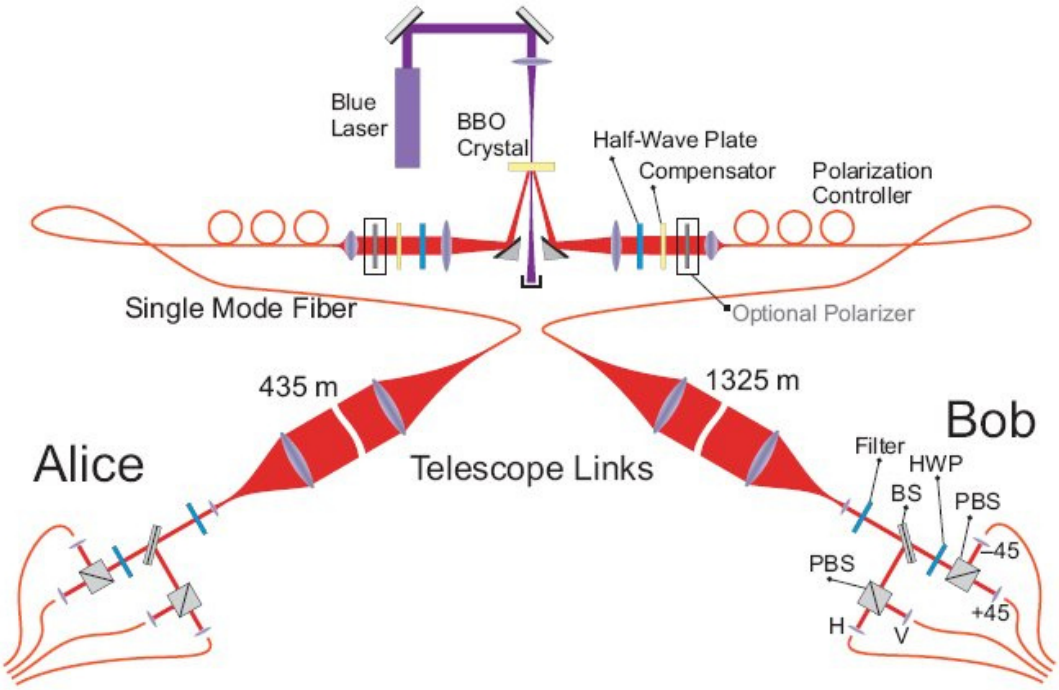


*Figure 2.19. The free-space entanglement system as implemented by the University of Waterloo. No direct line of site existed between Alice and Bob.*

In yet another free-space experiment, a team at the University of Erlangen along with collaborators at the Max-Planck institute for the science of Light and the Imperial College, London demonstrated the first free-space implementation of continuous variable quantum QKD [119]. The experiment ran over a 100m free-space link and used pin photodiodes for detectors, the first QKD system to do so.

Finally, the SECOQC collaboration ended with a conference and technology showcase in Vienna. In a real time video presentation, the SECOQC quantum network was demonstrated to the conference delegates [120]. The network (shown below in Figure 2.20) consisted of six nodes with eight links using standard telecommunications fibre and one free-space link. The demonstration also included an attempted eavesdropping on one of the nodes which was then discarded and alternative routing implemented by the network management layer. The conference also hosted the inaugural meeting of the European Telecommunication Standards Institute (ETSI) Industry Specification Group on Quantum Key Distribution and Quantum Technologies, charged with the setting of international standards for Quantum Information Technologies.

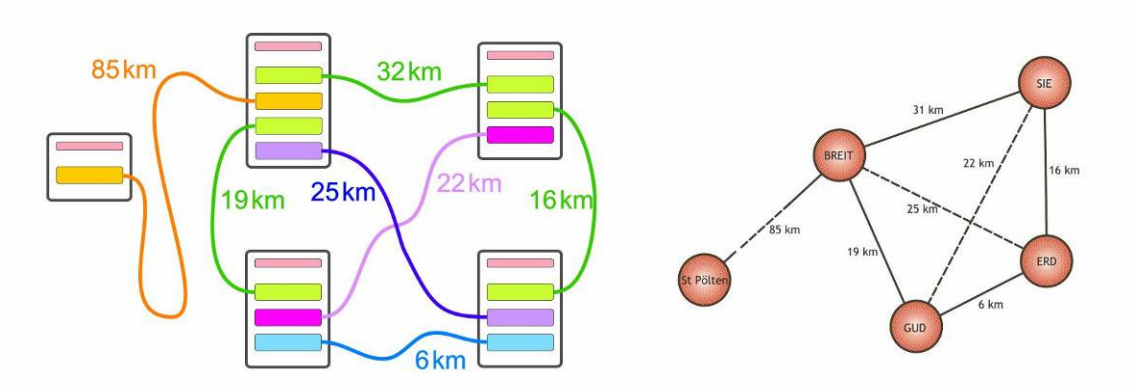


*Figure 2.20. Topographical representations of the SECOQC quantum network showing transmission distances and system architecture. The free-space node is not shown.*

## 2.7 Summary

In this chapter it has been shown how the idea of Quantum key distribution was originally conceived and then implemented. Also discussed was how the idea has broadened into a field of research perfecting what were, in fact, rather delicate, idiosyncratic experiments.

Currently systems are being reported with gigahertz clock rates operating over hundreds of kilometres in both fibre and free space. The diagram below shows the current state of the art in terms of transmission distance and bit rates. Sub-systems such as sources and detectors have received much attention and have improved in terms of speed, efficiency and size. Quantum key distribution has been demonstrated in networks and there are several commercial companies marketing quantum components and QKD systems.

## 2.8 The future

It seems certain that QKD will continue to evolve in terms of secure key bit rate and distance. However, the limits on transmission distances are approaching the physical limits of the available transmission technology (i.e. Fibre and free-space attenuation effects). Disregarding the development of future technologies such as quantum repeaters, in order to achieve a global reach it would appear the only place left to go is up. Several groups have already published details and feasibility studies [127] & [128] concerning space borne QKD experiments and systems. It also appears that at least one research collaboration is actively pursuing space borne system development [129].

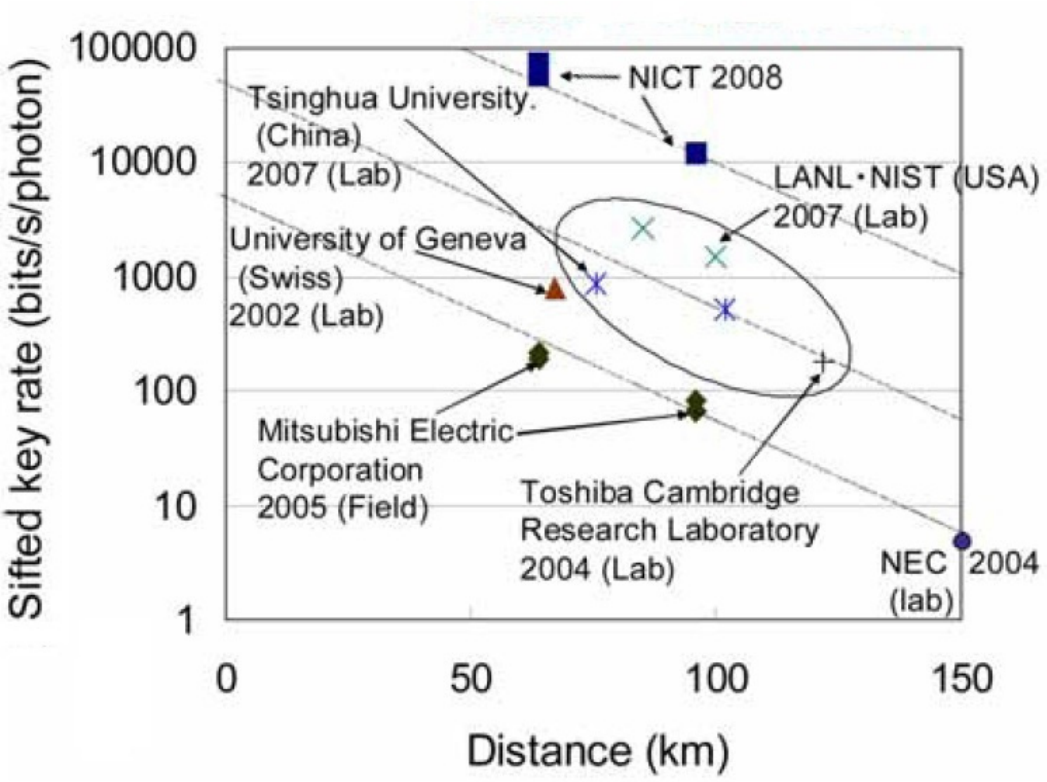


*Figure 2.21. Diagram showing the state of the art for QKD in terms of sifted key rate and transmission distances.*

Another interesting proposal comes from the air traffic control community where it has been proposed to use the commercial air transport network to both distribute keys and to improve air transport security [130]. This provides a viable alternative to spaceborne QKD systems and their associated complexity since it is a much shorter step to using the air transport network for key distribution on a global scale without the need for expensive satellite launch costs.

A list of QKD highlights for this period is shown below in Table 2.3.

| Year | Achievement |
|---|---|
| 2004 | 122km QKD in fibre<br>Entangled state QKD over 1.5km<br>GHz clocked free-space QKD<br>GHz clocked QKD over 10km of fibre<br>SECOQC collaboration starts |
| 2005 | BBN network with optical switching of QKD channels<br>Decoy state protocol in 20km of fibre<br>Continuous QKD in 20km of fibre<br>WDM QKD in 50km of fibre<br>QKD in 6.5km of fibre at 2GHz clock rate<br>Entangled state QKD over 7.8km<br>Entangled state QKD over 13km |
| 2006 | 2Mbits/s sifted key rates<br>TES detectors<br>184km QKD in fibre<br>DPS QKD over 100km<br>QKD at 3.3GHz clock rates<br>QKD over passive optical networks<br>Space division multiplexed (MIMO) QKD |
| 2007 | Entanglement based QKD over 144km in free-space<br>Decoy state QKD over 144km in free-space<br>Entanglement based DPS QKD<br>DPS QKD over 40km of fibre, QKD over 200km<br>Use of Niobium Nitride superconducting detectors<br>Continuous decoy state QKD, QKD over PONs at 3GHz<br>Waveguide based entanglement sources |
| 2008 | QKD over 97km of telecommunications fibre<br>1Mbit/s key rates over 20km of fibre<br>Entanglement-based qkd over 100km of fibre<br>Daylight free-space entanglement based QKD<br>Entanglement based QKD with no direct line of sight<br>Free space continuous variable QKD<br>SECOQC demonstrates network based QKD<br>ETSI standards committee formed for Quantum information technologies |

*Table 2.3. A list of QKD research achievements 2004 – 2008.*

## 2.9 Chapter 2 references


[1] S Wiesner, “Conjugate coding”, ACM Sigact news, **15**, No.1, 76-88, (1983).

[2] C.H. Bennett, G. Brassard, “The dawn of a new era for quantum cryptography: the experimental prototype is working!”, ACM Sigact News, **20** (4), 78–80, (1989).

[3] J.E. Lilienfeld, “Method and apparatus for controlling electric current”, US patent 1745175, first filed in Canada on 22.10.1925.

[4] O. Heil, “Improvements in or relating to electrical amplifiers and other control arrangements and devices”, GB patent 439457, first filed in Germany on March 2, 1934.

[5] R.G. Arns, “The other transistor: early history of the metal–oxide–semiconductor field-effect transistor”, Engineering Science and Education Journal **7**, 5, 233 – 240, (Oct 1998).

[6] A Einstein, “Zur Quantentheorie der Strahlung”, Physikalische Zeitschrift, **18**, 121-128, (1917).

[7] A.L. Schawlow and C.H. Townes, "Infrared and Optical Masers," Phys. Rev. **112**, 1940, (1958).

[8] M.O. Rabin, “How to exchange secrets with oblivious transfer”, Technical report TR-81, Aiken computation laboratory, Harvard University, (1981).

[9] C.H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, “Quantum Cryptography, or Unforgeable Subway Tokens”, Advances in Cryptography: Proceedings of Crypto 82, Plenum (New York), 267-275, (1983).

[10] C.H. Bennett, G. Brassard, “Quantum cryptography and its application to provably secure key expansion and coin tossing”, IEE International Symposium on Information Theory, St. Jovite, Quebec. (1983).

[11] C.H. Bennett, G. Brassard, “Quantum cryptography: Public key cryptography and coin tossing”, International conference on computers, systems and signal processing, Bangalore, India. December 10-12, 175 – 179, (1984).

[12] G. Brassard, “Brief History of Quantum Cryptography: A Personal Perspective”, Proceedings of the IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, Awaji Island, Japan, (17 October 2005).

[13] J. Smolin, “Early Days of Experimental Quantum Cryptography”, IBM J. Res. & Dev. **48** No. 1, (2004).

[14] C.H. Bennett, F. Bessette, G. Brassard. L. Salvail. & J. Smolin, “Experimental Quantum Cryptography”, Journal of Cryptology **5**, 1, 3-28, (1992).

[15] A.K. Ekert, “Quantum cryptography based on bells theorem”, Phys Rev Lett. **67**(6) 661-663 (1991).

[16] A. Aspect, P. Grangier, and G. Roger, “Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities”, Phys. Rev. Lett. **49**, 91 – 94, (1982).

[17] A. Aspect, J. Dalibard, G. Roger, “Experimental test of Bell's inequalities using time-varying analyzers”, Phys. Rev. Letters **49** 25, 1804, (1982).

[18] A.K. Ekert, Cracking codes, part II, +Plus magazine page7, Millennium Mathematics Project, University of Cambridge (2005).

[19] A.K. Ekert, J.G. Rarity, P.R. Tapster, and G.M. Palma, “Practical quantum cryptography based on two-photon interferometry”, Phys. Rev. Lett. **69**, 1293–1296, (1992).

[20] J.G. Rarity, & P.R. Tapster, “Experimental violation of Bell's inequality based on phase and momentum”, Phys. Rev. Lett. **64**, No. 21. 1293–1295, (1990).

[21] J.G. Rarity, P.R. Tapster, E. Jakeman, T. Larchuk, R.A. Campos, M.C. Teich, & B.E.A. Saleh, “Two photon interference in a Mach-Zhender interferometer”, Phys. Rev. Lett. **65**, 1293–1295, (1990).

[22] S.F. Seward, P.R. Tapster, J.G. Walker, & J.G. Rarity, “Daylight demonstration of low light level communication system using correlated photon pairs”, Quantum Opt. **3** 201-207, (1991).

[23] C.H. Bennett, “Quantum cryptography using any two nonorthogonal states”, Phys. Rev. Lett., **68** (21), 3121–3124, (1992).

[24] A. Muller, J. Breguet, and N. Gisin, “Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over More than 1 km”, Europhys. Lett. **23**, 383, (1993).

[25] P.D. Townsend, J.G. Rarity and P.R. Tapster, “Enhanced single photon fringe visibility in a 10km-long prototype quantum cryptography channel”, Electronics. Letters, **29** 1291-1293, (1993).

[26] P.D. Townsend, J.G. Rarity and P.R. Tapster, “Single photon interference in 10km long optical fibre interferometer”, Electronics Letters, **29** 634-635, (1993).

[27] P.D. Townsend, “Secure key distribution system based on quantum cryptography” Electronics Letters, **30,** 809-811, (1994).

[28] J.D. Franson and H. Ilves, “Quantum cryptography using optical fibers”, Applied Optics, **33**, 14, 2949-2954, (1994).

[29] J.D. Franson and B.C. Jacobs, “Operational system for quantum cryptography”, Electronics Letters **31**, 232-234, (1995).

[30] C.H. Bennett, G. Brassard, and J-M. Robert, “Privacy Amplification by Public Discussion”, SIAM J. Comput. **17**, 2, 210-229, (1988).

[31] C. Marand and P.D. Townsend, “Quantum key distribution over distances as long as 30 km”, Opt. Lett. **20**, 1695-1697, (1995).

[32] A. Muller, H. Zbinden and N. Gisin, “Quantum cryptography over 23 km in installed under-lake telecom fibre”, Europhys. Lett., **33,** 5, 335-339 (1996).

[33] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, “Plug and play’’ systems for quantum cryptography, Appl. Phys. Lett., **70**, 7, (1997).

[34] L. Goldenburg & L. Vaidman, “Quantum cryptography based on orthogonal states”, Phys. Rev. Lett. **75**, 7, 1239-1243, (1995).

[35] P.G. Kwiat, K. Mattle, H. Weinfurter, and A. Zeilinger, “New High-Intensity Source of Polarization-Entangled Photon Pairs”, Phys. Rev Lett. **75**, 4337, (1995).

[36] J. Franson, and B. Jacobs, “Quantum cryptography in free-space”, Optics Letters **21**, 1854–1856, (1996).

[37] W.T. Buttler, R.J. Hughes, P.G. Kwiat, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, and C.M. Simmons, “Free space quantum key distribution”, Physical Review A **57**, 2379–2382, (1998).

[38] H. Zbinden, J.D. Gautier, N. Gisin, B. Huttner, A. Muller, W. Tittel, “Interferometry with Faraday mirrors for quantum cryptography”, Electronics Letters, **33**, (7), 586 – 588, (1997).

[39] P.D. Townsend, “Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing”, Electronics Letters, **33**, 3, 188-190, (1997).

[40] P.D. Townsend, “Quantum cryptography on multi-user optical fibre networks”, Nature, **385**, 47, (1997).

[41] J.S. Bell, “On the problem of hidden variables in quantum mechanics”, Reviews of Modern Physics, 38 (3), pages 447–452, (1966).

[42] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, “Violation of Bell's Inequality under Strict Einstein Locality Conditions”, Phys. Rev. Lett. **81**, 5039–5043, (1998).

[43] W.T. Buttler, R.J. Hughes, P.G. Kwiat, S.K. Lamoreaux, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson and C.M. Simmons, “Practical free-space quantum key distribution over 1 km”, Phys. Rev. Lett. (USA) **81** 3283-6, (1998).

[44] Esprit Project 28139 EQCSPOT, Single Photon Optical Technologies Cordis archive page: URL: http://cordis.europa.eu/esprit/src/28139.htm (2001).

[45] M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren, and E. Sundberg, “Experiments on long wavelength (1550 nm) "plug and play" quantum cryptography systems”, Optics Express, **4**, Issue 10, 383-387. (1999).

[46] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, “Quantum Cryptography with Entangled Photons”, Phys. Rev. Lett. **84**, 4729–4732, (2000).

[47] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, “Quantum Cryptography Using Entangled Photons in Energy-Time Bell States”, Phys. Rev. Lett. **84**, 4737, (2000).

[48] D.S. Naik, C.G. Peterson, A.G. White, A.J. Berglund, and P.G. Kwiat, “Entangled State Quantum Cryptography: Eavesdropping on the Ekert Protocol”, Phys. Rev. Lett. **84**, 4733–4736, (1999).

[49] W.T. Buttler, R.J. Hughes, S.K. Lamoreaux, G.L. Morgan, J.E. Nordholt and C.G. Peterson, “Daylight quantum key distribution over 1.6 km”, Phys. Rev. Lett. (USA) **84** 5652-5 (2000).

[50] R.J. Hughes, G.L. Morgan and C.G. Peterson, “Quantum key distribution over a 48 km optical fibre network”, Journal of Modern Optics, **47**, No. 23, 533 – 547, (2000).

[51] R.J. Hughes, W.T. Buttler, P.G. Kwiat, S.K. Lamoreaux, G.L. Morgan, J.E. Nordholt, and C.G. Peterson, “Quantum Cryptography For Secure Satellite Communications”, IEEE Aerospace 2000 Conference, Big Sky, Montana, (2000).

[52] P.M. Gorman, P.R. Tapster and J.G. Rarity, “Secure Free-space Key Exchange Over a 1.2 km Range Using Quantum Cryptography”, CLEO/Europe-IQEC, 10-15 September 2000.

[53] G. Ribordy, J. Brendel, J-D. Gautier, N. Gisin, and H. Zbinden, “Long-distance entanglement-based quantum key distribution”, Physical Review A, **63**, 012309, (2000).

[54] Corning, SMF-28e® optical fiber product information _PI1344, URL:http://www.corning.com/assets/0/433/573/583/09573389-147D-4CBC-B55F-18C817D5F800.pdf (2007).

[55] Project IST-1999-100 33: QuComm, Long Distance Photonic Quantum Communication project homepage: URL:http://www.imit.kth.se/QEO/qucomm/index.html.

[56] J.G. Rarity, P.R. Tapster, and P.M. Gorman, “Free-space key exchange to 1.9 km and beyond”, J. Mod. Opt. **48**, 1887–1901, (2001).

[57] S. Tanzilli, H. De Riedmatten, H. Tittel, H. Zbinden, P. Baldi, M. De Micheli, D.B. Ostrowsky, N. Gisin, “Highly efficient photon-pair source using periodically poled lithium niobate waveguide”, Electronics Letters, **37**, 28, (2001).

[58] D.S. Bethune and W.P. Risk, “Autocompensating quantum cryptography”, New J. Phys. **4** 42, (2002).

[59] R.J Hughes, J.E Nordholt, D. Derkacs and C.G Peterson, “Practical free-space quantum key distribution over 10 km in daylight and at night”, New J. Phys. **4** 43, (2002).

[60] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P.M. Gorman, P.R. Tapster, and J.G. Rarity, “Quantum cryptography: A step towards global key distribution”, Nature **419**, 450, (2002).

[61] D Stucki, N Gisin, O Guinnard, G Ribordy and H Zbinden, “Quantum key distribution over 67 km with a plug & play system”, New Journal of Physics **4** 41.1–41.8, (2002).

[62] First commercial company offering Quantum Cryptography products, ID Quantique URL: http://www.idquantique.com/home.htm.

[63] F. Grosshans and P. Grangier, “Continuous Variable Quantum Cryptography Using Coherent States”, Phys. Rev. Lett. **88**, 057902, (2002).

[64] M.C. Booth, M. Atatüre, G. Di Giuseppe, B.E.A. Saleh, A.V. Sergienko and M.C. Teich, “Counterpropagating entangled photons from a waveguide with periodic nonlinearity”, Physical Review A, **66**, 023815, (2002).

[65] J.G Rarity, P.R Tapster, P.M Gorman and P. Knight, “Ground to satellite secure key exchange using quantum cryptography”, New Journal of Physics **4** 82.1–82.21, (2002).

[66] ESA QSPACE Final reports: M. Aspelmeyer, H. Böhm, C. Brukner, R. Kaltenbaek, M. Lindenthal, J. Petschinka, T. Jennewein, R. Ursin, P. Walther, A. Zeilinger, M. Pfennigbauer, W. Leeb, "Quantum Communications in Space", ESTEC, 16358/02/NL/SFe, (2003). J.G. Rarity, P.M. Gorman, P.R. Tapster, B. Lowans, P. Knight, C. Kurtsiefer and H. Weinfurter., "Quantum Communications in Space", ESTEC 16441/02/NL/Sfe, (2003).

[67] P. Toliver, R.J. Runser, T.E. Chapuran, J.L. Jackel, T.C. Banwell, M.S. Goodman, R.J. Hughes, C.G. Peterson, D. Derkacs, J.E. Nordholt, L. Mercer, S. McNown, A. Goldman, J. Blake, "Experimental investigation of quantum key distribution through transparent optical switch elements", IEEE Photonics Technology Letters, **15**, 11, 1669-1671, (2003).

[68] H. Kosaka, A. Tomita, Y. Nambu, T. Kimura, K. Nakamura, "Single-photon interference experiment over 100 km for quantum cryptography system using a balanced gated-mode photon detector", Electronics Letters, **39**, No. 16, 1199-1201, (2003).

[69] T. Hasegawa, T. Nishioka, H. Ishizuka, J. Abe, M. Matsui, and S. Takeuchi, "Experimental realization of quantum cryptosystem over 87km", Conference Paper, Quantum Electronics and Laser Science Conference (QELS) Cryptography and Novel Sources of Entangled Photons (QtuB), Baltimore, Maryland, (2003).

[70] A. Poppe, A. Fedrizzi, R. Ursin, H. Böhm, T. Lörunser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein and A. Zeilinger, "Practical quantum key distribution with polarization entangled photons", Optics Express, **12**, Issue 16, 3865-3871, (2004).

[71] C. Gobby, Z.L. Yuan, and A.J. Shields, "Quantum key distribution over 122 km of standard telecom fiber", Applied Physics Letters **84**, 3762–3764, (2004).

[72] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, K. Nakamura, "Single-photon interference over 150-km transmission using silica-based integrated-optic interferometers for quantum cryptography", Jpn. J. Appl. Phys.,**43** 9,L1217 - L1219, (2004).

[73] J. Bienfang, A.J. Gross, A. Mink, B.J. Hershman, A. Nakassis, X. Tang, R. Lu, D.H. Su, C.W. Clark, C.J. Williams, E.W. Hagley, and J. Wen, "Quantum key distribution with 1.25 Gbps clock synchronization", Optics Express **12**, 2011–2016, (2004).

[74] K.J. Gordon, V. Fernandez, P.D. Townsend, and G.S. Buller., "A Short Wavelength GigaHertz Clocked Fiber-Optic Quantum Key Distribution System", IEEE Journal of Quantum Electronics, **40** (7), 900-908, (2004).

[75] SECOQC project website, URL: http://www.secoqc.net/index.html.

[76] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, H. Yeh, "Current status of the DARPA Quantum Network" (Invited paper), SPIE Proceedings, VOL 5815, pages 138-149, (arxiv :quant-ph/0503058), (2005).

[77] Y. Zhao, B. Qi, X. Ma, H-K. Lo, L. Qian, "Experimental Quantum Key Distribution with Decoy States", Phys. Rev. Lett. **96**, 070502, (2006).

[78] W-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication", Phys. Rev. Lett. **91**, 057901, (2003).

[79] H-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution", Phys. Rev. Lett. **94**, 230504, (2005).

[80] X. Ma, B. Qi, Y. Zhao, and H-K. Lo, "Practical Decoy State for Quantum Key Distribution", Phys. Rev. A **72**, 012326, (2005).

[81] X-B. Wang, "A decoy-state protocol for quantum cryptography with 4 intensities of coherent states", http://arxiv.org/abs/quant-ph/0411047, (2005).

[82] X-B. Wang, "Beating the PNS attack in practical quantum cryptography", Phys. Rev. Lett., **94**, 230503, (2005).

[83] Z.L. Yuan and A.J. Shields, "Continuous operation of a one-way quantum key distribution system over installed telecom fibre", Optics Express **13**, 660-665, (2005).

[84] T.J. Xia, D.Z. Chen, G.A. Wellbrock, A. Zavriyev, A. Craig Beal, and K.M. Lee, "In-Band Quantum Key Distribution (QKD) on Fiber,Populated by High-Speed Classical Data Channels", Optical Fiber Communication Conference and Exposition (OFC), Anaheim, USA, (2006).

[85] Link to specification for ITU Grid C-Band DWDM 100GHz channel spacing. URL:http://www.fiberdyne.com/products/itu-grid.html

[86] K.J. Gordon, V. Fernandez, G.S. Buller, I. Rech, S.D. Cova and P.D. Townsend, "Quantum key distribution system clocked at 2 GHz, Optics Express", **13** (8), 3015-3020, (2005).

[87] K. Resch, M. Lindenthal, B. Blauensteiner, H. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, P. Walther, H. Weier, H. Weinfurter, and A. Zeilinger, "Distributing entanglement and single photons through an intra-city, free-space quantum channel", Opt. Exp. **13**, 202-209 (2005).

[88] C-Z. Peng, T. Yang, X-H. Bao, J. Zhang, X-M. Jin, F-Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, N. Li, B-L. Tian, and J-W. Pan, "Experimental Free-Space Distribution of Entangled Photon Pairs Over 13km: Towards Satellite-Based Global Quantum Communication", Phys. Rev. Lett. **94**, 150501, (2005).

[89] X. Tang, L. Ma, A. Mink, A. Nakassis, H. Xu, B. Hershman, J.C. Bienfang, D. Su, R.F. Boisvert, C.W. Clark, and C.J. Williams., "Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over Mbit/s", Opt. Exp., **14**, Issue 6, 2062-2070, (2006).

[90] D.J. Rogers, J.C. Bienfang, A. Mink, B.J. Hershman, A. Nakassis, X. Tang, L. Ma, D.H. Su, C.J. Williams, C.W. Clark, "Free-space quantum cryptography in the H-alpha Fraunhofer window", Free-Space Laser Communications VI. Proceedings of the SPIE, Volume 6304, 630417, (2006).

[91] P.A. Hiskett, D. Rosenberg, C.G. Peterson, R.J. Hughes, S. Nam, A.E. Lita, A.J. Miller and J.E. Nordholt, "Long-distance quantum key distribution in optical fibre", New Journal of Physics **8,** 193, (2006).

[92] K. Inoue, E. Waks and Y. Yamamoto, “Differential Phase Shift Quantum Key Distribution”, Phys. Rev. Lett. **8**9, 037902, (2002).

[93] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M.M. Fejer, K. Inoue and Y. Yamamoto, “Differential phase shift quantum key distribution experiment over 105 km fibre”, New J. Phys. **7,** 232, (2005).

[94] E. Diamanti, H. Takesue, C. Langrock, M.M. Fejer and Y. Yamamoto, “100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors”, Optics Express, **14**, 26, (2006).

[95] K.J. Gordon, V. Fernandez, R.J. Collins, I. Rech, S.D. Cova, P.D. Townsend and G.S. Buller, “3.3 Gigahertz Clocked Quantum Key Distribution System”, Presented at ECOC 05, Glasgow, UK, (2005).

[96] V. Fernandez, R.J. Collins, K.J. Gordon, P.D. Townsend and G.S. Buller, “Gigahertz Clocked Quantum Key Distribution in Passive Optical Networks”, IEEE LEOS Summer Topical 2006. Quantum Communications in Telecom Networks, Quebec City, Canada, July 17-19 2006

[97] M. Gabay and S. Arnon, “Quantum Key Distribution by a Free-Space MIMO System”, Journal of Lightwave Technology, **24**, 8, (2006).

[98] K. Inoue, T. Honjo and H. Takesue, “Differential-phase quantum key distribution experiment using a series of quantum entangled photon pairs”, Optics Letters, **32**, 9, (2007).

[99] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter & A. Zeilinger, “Entanglement-based quantum communication over 144 km”, Nature Physics **3**, 481 – 486, (2007).

[100] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger and H. Weinfurter, “Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km”, Phys. Rev. Lett. **98**, 010504, (2007).

[101] N. Namekata, G. Fujii, S. Inoue, T. Honjo and H. Takesue, “Differential phase shift quantum key distribution using single-photon detectors based on a sinusoidally gated InGaAs/InP avalanche photodiode”, Applied Physics Letters **91**, 011112, (2007).

[102] H. Takesue, S.W. Nam, Q. Zhang, R.H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, “Quantum key distribution over 40 dB channel loss using superconducting single photon detectors”, Nature Photonics **1**, 343, (2007).

[103] J.F. Dynes, Z.L. Yuan, A.W. Sharpe, and A.J. Shields, “Practical quantum key distribution over 60 hours at an optical fiber distance of 20km using weak and vacuum decoy pulses for enhanced security”, Optics Express, **15**, 13, 8465-8471, (2007).

[104] V. Fernandez, R.J. Collins, K.J. Gordon, P.D. Townsend, and G.S. Buller, “Passive Optical Network Approach to GigaHertz-Clocked Multi-user Quantum Key Distribution”, IEEE Journal of Quantum Electronics, **43**, 2, (2007).

[105] M. Fiorentino, S.M. Spillane, R.G. Beausoleil, T.D. Roberts, P. Battle, and M.W. Munro, “Spontaneous parametric down-conversion in periodically poled KTP waveguides and bulk crystals”, Optics Express, **15**, 12 747911, (2007).

[106] O. Kuzucu and F.N.C. Wong, “Narrowband Pulsed Polarization-Entangled Photon Source for Free-Space Quantum Key Distribution”, Conference Paper, Quantum Electronics and Laser Science Conference (QELS), Baltimore, Maryland, (May 6, 2007).

[107] Q. Zhang, H. Takesue, C. Langrock, X. Xie, M.M. Fejer, Y. Yamamoto, “Hong-Ou-Mandel dip using photon pairs from a PPLN waveguide”, Conference Paper, Quantum Electronics and Laser Science Conference (QELS), San Jose, California, (May 4, 2008).

[108] G. Fujii, N. Namekata, M. Motoya, S. Kurimura and S. Inoue, “Bright narrowband source of photon pairs at optical telecommunication wavelengths using a type-II periodically poled Lithium Niobate waveguide”, Optics Express, **15**, 20, 12772 – 12776, (2007).

[109] S. Odate, A. Yoshizawa and H. Tsuchida, “Polarisation-entangled photon-pair source at 1550nm using 1 mm-long PPLN waveguide in fibre-loop configuration”, Electronics Letters **43** 24, (2007).

[110] A. Yoshizawa, R. Kaji and H. Tsuchida, “Two-photon Interference at 1550 nm Using Two Periodically Poled Lithium Niobate Waveguides”, Jpn. J. Appl. Phys. **42** 5652-5653, (2003).

[111] P. Trojek, C. Schmid, M. Bourennane, H. Weinfurter & C. Kurtsiefer, “Compact source of polarization-entangled photon pairs”, Optics Express, **12**, 2, (1994).

[112] M. Fiorentino, C.E. Kuklewicz, and F.N.C. Wong, “Source of polarization entanglement in a single periodically poled KTiOPO4 crystal with overlapping emission cones”, Optics Express, **13**, 1, 127-135, (2005).

[113] P.G. Kwiat, K. Mattle, H. Weinfurter, and A. Zeilinger, “New High-Intensity Source of Polarization-Entangled Photon Pairs”, Phys. Rev Lett. **75**, 4337, (1995).

[114] A. Tanaka, M. Fujiwara, S.W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K. Yoshino, S. Miki, B. Baek, Z. Wang, A. Tajima, M. Sasaki, and A. Tomita, “Ultra fast quantum key distribution over a 97km installed telecom fibre with wavelength division multiplexing clock synchronization”, Optics Express, **16**, Issue 15, 11354-11360, (2008).

[115] Z.L. Yuan, A.R. Dixon, J.F. Dynes, A.W. Sharpe, and A.J. Shields, “Gigahertz quantum key distribution with InGaAs avalanche photodiodes”, Appl. Phys. Lett. **92**, 201104, (2008).

[116] T. Honjo, S.W. Nam, H. Takesue, Q. Zhang, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, B. Baek, R. Hadfield, S. Miki, M. Fujiwara, M. Sasaki, Z. Wang, K. Inoue and Y. Yamamoto, “Entanglement-based BBM92 QKD experiment using superconducting single photon detectors”, Conference Paper: Quantum Electronics and Laser Science Conference (QELS), San Jose, California, (May 4, 2008).

[117] M. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares and C. Kurtsiefer, “Daylight operation of a free space entanglement-based quantum key distribution system”, New Journal of Physics **11** 045007, (2009).

[118] C. Erven, C. Couteau, R. Laflamme, and G. Weihs, “Entangled quantum key distribution over two free-space optical links”, Optics Express, **16**, 21, 16840-16853, (2008).

[119] D. Elser, T. Bartley, B. Heim, Ch. Wittmann, D. Sych and G. Leuchs, “Feasibility of free space quantum key distribution with coherent polarization states”, New J. Phys. **11** 045014, (2009).

[120] SECOQC press release: Presentation of the SECOQC-Network in Vienna, http://www.secoqc.net/downloads/pressrelease/SECOQC_PRESS%20RELEASE_english.pdf.

[121] M. Sasaki, “Toward New Generation Quantum Cryptography - Japanese strategy”, (Invited paper), IST-SECOQC conference, Vienna, October 8-10, 2008. URL:http://www.secoqc.net/html/conference/schedule.html.

[122] B. Cabrera, R.M. Clarke, P. Colling, A.J. Miller, S. Nam, and R.W. Romani, “Detection of single infrared, optical, and ultraviolet photons using superconducting transition edge sensors”, Applied Physics Letters **73**, 6, (1998).

[123] A.P. VanDevender and P.G. Kwiat, “High Efficiency Single Photon Detection via Frequency Up-Conversion”, Journal of Modern Optics, **51**, Issue 9 & 10 1433 – 1445, (2004).

[124] C. Langrock, E. Diamanti, R.V. Roussev, Y. Yamamoto, and M.M. Fejer, “Highly efficient single-photon detection at communication wavelengths by use of upconversion in reverse-proton-exchanged periodically poled LiNbO3 waveguides”, Optics Letters **30**, 13, (2005).

[125] R.T. Thew, S. Tanzilli, L. Krainer, S.C. Zeller, A. Rochas, I. Rech, S. Cova, H. Zbinden and N. Gisin, “Low jitter up-conversion detectors for telecom wavelength GHz QKD”, New Journal of Physics **8,** 32, (2006).

[126] H. Kamada, M. Asobe, T. Honjo, H. Takesue, Y. Tokura, Y. Nishida, O. Tadanaga, and H. Miyazawa, “Efficient and low-noise single-photon detection in 1550 nm communication band by frequency upconversion in periodically poled $LiNbO_3$ waveguides”, Optics Letters, **33**, 7, 639-641, (2008).

[127] R.J. Hughes, W.T. Buttler, P.G. Kwiat, S.K. Lamoreaux, G.L. Morgan, J.E. Nordholt, and C.G. Peterson, “Quantum Cryptography For Secure Satellite Communications”, IEEE Aerospace 2000 Conference, Big Sky, Montana, (14-25/3/2000).

[128] J.G. Rarity, P.R. Tapster, P.M. Gorman and P. Knight, “Ground to satellite secure key exchange using quantum cryptography”, New Journal of Physics **4** 82.1–82.21, (2002).

[129] J.M. Perdigues Armengol, B. Furch, C.J. de Matos, O. Minstera, L. Cacciapuotia, M. Pfennigbauer, M. Aspelmeyer, T. Jennewein, R. Ursin, T. Schmitt-Manderbach, G. Baister, J. Rarity, W. Leeb, C. Barbieri, H. Weinfurter, and A. Zeilinger, “Quantum communications at ESA: Towards a space experiment on the ISS”, Acta Astronautica, **63**, Issues 1-4, 165-178, (July-August 2008).

[130] M. Riguidel, “Quantum Crypt: Enhancement of AGT Communications Security using Quantum Cryptography”, European Organisation for the Safety of Air Navigation (EUROCONTROL), ENST/EEC/QC.12.01.WP3.A, pages71-100, (2005).

# Chapter 3 – Some considerations for practical QKD systems

## 3.1 Introduction

The purpose of this chapter is to provide a theoretical toolkit with which to understand some of the issues involved in building a reasonably secure QKD system. Whilst this thesis is mainly concerned with free-space QKD, many concepts have application to all types of QKD system and therefore are worthy of consideration.

Firstly it is necessary to understand the basis of the security of QKD. This requires a basic understanding of quantum information coding, the quantum mechanical basis of conjugate coding and some of the rules and protocols that allow the method to work in practice.

Secondly, this chapter discusses some of the engineering problems and constraints imposed by the above. These include, for instance, the generation of single photons (or a reasonable facsimile thereof), the problems associated with the transmission of light through a medium and the generation of random numbers. Lastly, some of the technologies available for the detection of single light quanta are considered.

## 3.2 The physical basis for QKD[2]

Quantum key distribution (QKD) is now regarded as one of a variety of applications of quantum information processing (QIP). Like all of the prospective applications in the field its operation is intimately connected with some of the basic phenomena of QM, specifically:

- The postulates of Quantum mechanics
- The principle of superposition
- The uncertainty principle
- No cloning theory
- Conjugate coding

The following section attempts to provide some familiarity with these concepts and how they relate to QKD.

[2] This part of the thesis relies heavily on references [1] to [4]. In some cases, such as the QM postulates, [2] is quoted verbatim because, in the author's opinion, Nielsen and Chuang express the concept better (in a QIP context) than anyone else.

### *3.2.1 The postulates of quantum mechanics*

Quantum mechanics is based on a set of postulates which cannot be derived analytically but nonetheless provide an extremely accurate framework for describing quantum processes.

#### *3.2.1.1 Postulate 1. The state representation.*

"Associated with any isolated physical system is a complex vector space with inner product (a Hilbert space) known as the state space of the system. The physical state of the system is completely described by its state vector, which is a unit vector in the system's state space".

***Superposition and representation of Qubits***

In classical information processing, the fundamental unit of information is the binary digit or Bit. By analogy, QIP applications use an entity known as a qubit. Now, whilst the classical bit can take on two values, 0 or 1, the qubit can take on the value of 0 or 1 or a superposition of both values.

A way of physically representing the qubit given that it represents a range of possible values between two base values might be to use a two level quantum mechanical system with two arbitrary orthogonal base states. Examples of two such systems are shown below in Figure 3.1.

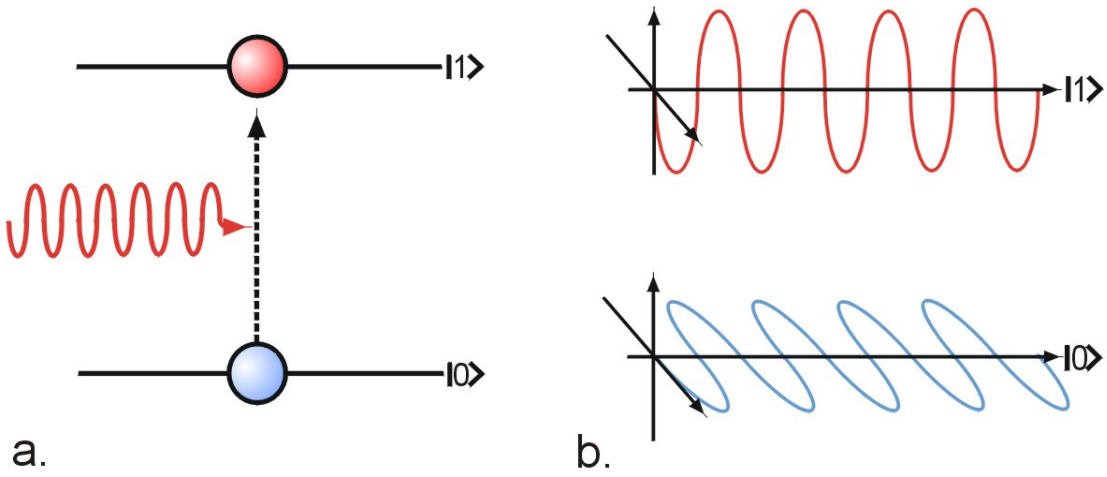


*Figure 3.1. Possible representations of two level systems.* ***a****. shows an atom system with an electron in the ground state representing the state* $|0\rangle$*, whilst the excited state represents the state* $|1\rangle$*.* ***b****. In this case photon polarisation is used to depict the state with vertical representing* $|1\rangle$ *and horizontal polarisation representing the state* $|0\rangle$*.*

These base states are written as $|0\rangle$ or $|1\rangle$ (in the conventional bra-ket notation developed by Dirac) and are called the computational bases.

An arbitrary state of a qubit can then be represented by a linear superposition of these two basis states and written thus:

$$\psi = \alpha|0\rangle + \beta|1\rangle \qquad (3.1)$$

Where $|\alpha|^2 + |\beta|^2 = 1$

This expression describes the most general state of a two level quantum mechanical system with $\alpha$ and $\beta$ as complex probability amplitudes representing the probability of measuring the qubit in the respective state. The 0 & 1 values are known as the eigenvalues corresponding to eigenvectors, $|0\rangle$ and $|1\rangle$, of the operator (e.g. polarisation) defining the measurement. When making a measurement in a particular basis, the measurement will always return one or other of the eigenvalues (or base states). The arbitrary state, $\psi$, can also be expressed by plotting it in a 2-dimensional complex space (known as a Hilbert space) as shown below in Figure 3.2. Measurements can be made on the state by projecting the vector (or one-dimensional subspace) onto the set of computational bases.

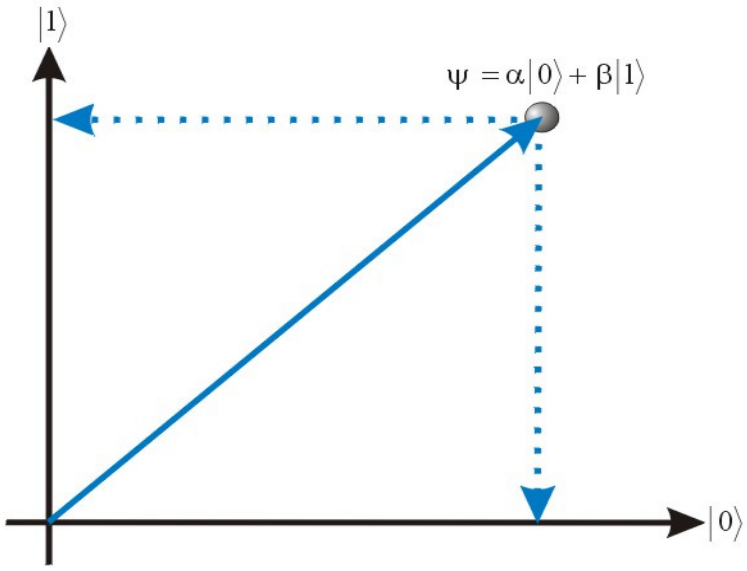


*Figure 3.2. The most general expression of an arbitrary qubit, $\psi$, written in terms of a vector with two base states $|0\rangle$ and $|1\rangle$ and their associated probability amplitudes, $\alpha$ & $\beta$. The complex state space used to display this vector is called a 2-dimensional Hilbert space and base states form a pairs of orthogonal vectors.*

In the diagram above, using a standard measurement basis one might expect a measurement outcome of *0* with a probability of $|\alpha|^2$, whereas one would expect the outcome to be *1* with a probability of $|\beta|^2$, since, when making a measurement, the system must eventually register a *0* or a *1*.

Importantly, one does not know anything about the state until it is measured, and even then ones knowledge is restricted to a statistical likelihood of a particular outcome.

***The Bloch Sphere***

The two-dimensional Hilbert space that is used to describe the vector space associated with qubit states can be projected onto the surface of a sphere. This sphere, known as a Bloch sphere, can be regarded as a geometrical representation of the complete state space of a single qubit and is extremely useful in visualising qubit states and operations on them. An example of the Bloch sphere with an arbitrary pure qubit state is shown below in Figure 3.3.

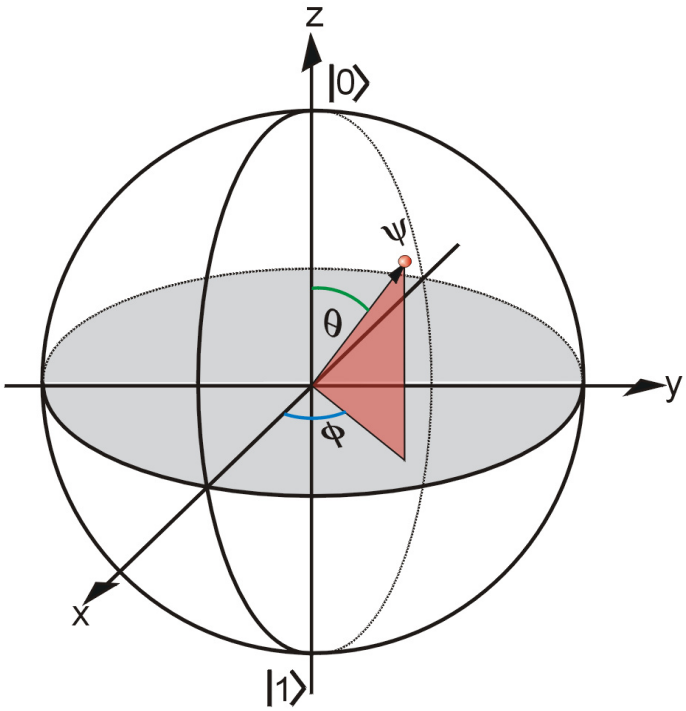


*Figure 3.3. The Bloch sphere with an arbitrary quantum state, ψ, as a point on its surface. The Bloch sphere can represent quantum states, and operations on them in a simple intuitive way. Antinodal points on the Bloch sphere are actually represented by orthogonal vectors in the 2-dimensional Hilbert space whilst different axes represent mutually exclusive (or conjugate) bases of a particular state space.*

A pure qubit state such as that written in Equation 3.1 and shown above in Figure 3.3 can be rewritten as:

$$\psi = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right) \qquad (3.2)$$

$$\text{with } \frac{-\pi}{2} \le \theta \le \frac{\pi}{2} \text{ and } 0 \le \phi \le \pi$$

It should be made clear here that the factor $e^{i\gamma}$ is a global phase which has no observable effects.

Therefore one can write:

$$\psi = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \qquad (3.3)$$

Incidentally, the classical bits *0* and *1* would reside at the north and south pole of the Bloch sphere respectively. In the polarisation domain, the Bloch sphere is analogous to the Poincare sphere with right and left circular polarisations at the poles and linear states around the equator.

#### *3.2.1.2 Postulate 2. Evolution of the state*

"The evolution of a closed quantum system is described by a unitary transformation. The state vector $|\psi\rangle$ of a system at time $t_1$ is related to its state vector $|\psi'\rangle$ at time $t_2$ by a unitary operator U which depends only on the times $t_1$ and $t_2$,

$$|\psi'\rangle = U|\psi\rangle \qquad (3.4)$$

Unitary transformations are linear transformations which operate on a complex space preserving lengths of vectors and angles between them. Any unitary transformation may act upon the state space of a single qubit."

This postulate allows the modelling of the evolution of a state under the influence of linear operators. For a single state system, these operators are generally 2×2 Hermitian (or self-adjoint) matrices having real eigenvalues and orthogonal eigenvectors. Furthermore the action of these operators is reversible.

#### *3.2.1.3 Postulate 3. Measurement*

"Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment.

If the state of the system before the measurement is $|\psi\rangle$, the probability that result m occurs is given by:

$$p_m = \langle\psi|M_m^\dagger M_m|\psi\rangle \qquad (3.5)$$

and the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} \qquad (3.6)$$

The measurement operators satisfy the completeness equation

$$\sum_m M_m^\dagger M_m = I \qquad (3.7)$$

i.e. The sum of probabilities of all outcomes must be 1."

This postulate implies that the measurement outcomes will always and only be eigenvalues of the operator used to make the measurement. Furthermore, once measured the system will assume the state that was measured so that another measurement made *immediately* afterward will yield the same result. The state will then continue to evolve from the measured value. In this way the act of measurement can be said to have perturbed the system. Incidentally, this postulate describes what is sometimes called "the collapse of the wavefunction", a notion which is still very much subject of debate.

***The Uncertainty principle***

An important part of the measurement process in QM is an understanding of the uncertainty principle. Uncertainty is a fundamental part of the formulation of QM. Specifically, the Heisenberg uncertainty principle [5], [6] (or perhaps, more accurately, the uncertainty relation) states that there are certain pairs of physical properties for which values cannot be known to arbitrary accuracy for both at the same time.

Furthermore, this measurement inaccuracy is not the result of the quality of the measurement instrumentation or even the result of perturbation by the measurement itself but a fundamental feature of the properties themselves.

The particular pairs of properties are known as canonically conjugate variables or non-commuting variables and are mathematically related to one another in such a way that knowledge of one limits the knowledge gained about the other. An example of this would be the light output from a laser. A c.w. laser emits at a particular wavelength and the longer it emits, the better one can define the wavelength. Conversely, if the laser were to emit a femto-second pulse there is a limit to the accuracy that one can define the wavelength. Common examples of conjugate variables include the position and momentum of a moving particle or the polarisation of a photon measured in non-orthogonal bases.

***Conjugate coding***

In his original paper [7] Wiesner points out that there are certain pairs of physical properties, simultaneous knowledge of which is impossible, that knowledge of one randomises knowledge of the other. Wiesner then goes on to extend this idea to conjugate basis sets in a Hilbert space.

The important point is that a state vector which is a linear superposition of two orthogonal base states in one Hilbert space cannot be measured unambiguously in another incompatible set of base states. In a way, Wiesner's insight restates part of the uncertainty principle and can be used for coding in QKD applications.

***The No cloning theorem***

The ability to clone an arbitrary quantum state with no previous knowledge of that state would allow several things to happen. For instance, such a capability would allow violation of the uncertainty principle in that an observer could make several versions of the state to be measured and then measure different aspects of the state simultaneously. In a QKD context this ability would render a QKD system insecure simply because an eavesdropper would be able to construct a machine to receive, clone and retransmit all of the signal states transmitted by Alice to Bob. In a somewhat more exotic fashion, quantum cloning would allow the possibility of superluminal communication [8].

Conveniently (for QKD), it turns out that such a device is impossible to construct. In their 1982 paper [9] Wooters and Zurek showed that such a machine is impossible, at least, for arbitrary states. The proof, after [2], page 532, proceeds as follows:

Suppose one wanted to create a copy of an unknown quantum state, one might invent a machine with two slots, slot A into which the unknown state, $|\psi\rangle$, to be copied is inserted, and slot B into which a blank state, $|s\rangle$, is inserted. The initial state of the quantum copying machine is then:

$$|\psi\rangle \otimes |s\rangle \qquad (3.8)$$

A unitary evolution now makes the copying procedure such that:

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \qquad (3.9)$$

Now suppose one repeats the copying procedure on another state, φ then one obtains:

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \qquad (3.10)$$

$$U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle \qquad (3.11)$$

Taking the inner product of the two equations gives:

$$\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2 \qquad (3.12)$$

However, $x = x^2$ has two solutions, x = 0 or x = 1, therefore either $|\psi\rangle = |\varphi\rangle$ or $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal. Therefore a quantum cloning machine can only clone orthogonal states and the cloning of non-orthogonal states is impossible. An interesting commentary on the no-cloning theory is given in [10].

### *3.2.2 Application to QKD*

The above applies to QKD in several ways. Firstly, it allows Alice to prepare a string of quantum states using photon polarisation in two bases of two values.

A rectilinear basis consisting of horizontal and vertically polarised states and a diagonal basis consisting of -45/+45 degree polarisation states. These two bases are conjugate and therefore if an incorrect basis is chosen in which to measure the states, no information will be recovered from the measurement. Conversely, use of the correct basis for a measurement will yield the correct values subject only to errors introduced by flaws in the optics, detectors and the transmission channel.

Secondly, if an eavesdropper is present and attempts to steal some of the states and make a measurement, not only will the results provide no information, but the eavesdropper will introduce errors into the transmission which can be detected by Alice and Bob. Furthermore, any attempt to clone the stolen states will also result in increased errors and likely detection.

#### *3.2.2.1 Measurements*

In a polarisation encoded QKD system, measurements are made by optical detectors using a polarisation analyser set in an appropriate orientation. A typical measurement arrangement is shown below.

In example **a.** a photon polarised at $45^{o}$ (in the diagonal basis) is incident on the polarising beamsplitter. Because the beamsplitter is oriented to analyse photons in the rectilinear basis one cannot predict from which port of the beamsplitter the photon will emerge, only that it will emerge from one of them. In fact, over many trials the photon will emerge from each port 50% of the time, and thus reveal no information about its original state. However, once it emerges it stays in its "chosen" value with no recollection of its previous state.

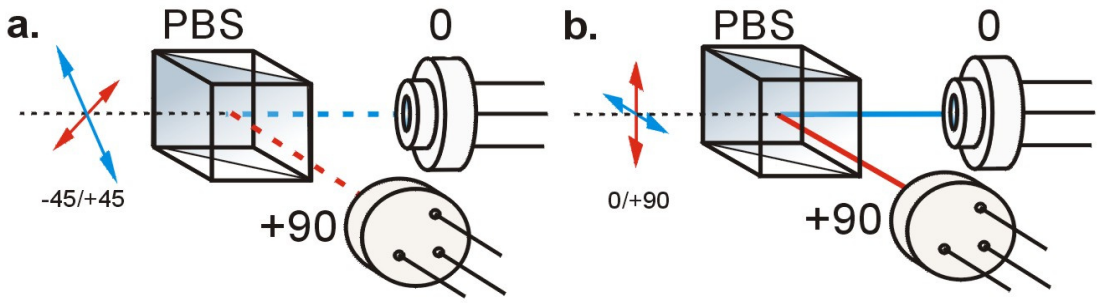


*Figure 3.4. A typical Bob detector element showing two detectors with a polarisation analyser.*

In **b.** the photon is polarised in the rectilinear basis and encounters a polarising beamsplitter oriented in the same basis. The result here is that the horizontal photon is reflected into the horizontal detector and the vertical photon impinges on the vertical detector making a correct measurement 100% of the time (subject to errors in optics etc.).

## 3.3 The BB84 key exchange protocol

### *3.3.1 Introduction*

Originally proposed by Charles Bennett and Gilles Brassard in 1983 [11] with subsequent modifications in 1984, the BB84 protocol was the first protocol designed to facilitate QKD [12] and uses conjugate variables such as those discussed above in section 3.2.1.3.

Since 1984 numerous other protocols have been proposed and implemented but BB84 and its variations remain the most popular key exchange protocol, certainly in free-space QKD. This protocol is also used exclusively by QKD systems described in this thesis. The basic arrangement for key exchange is shown in Figure 3.5 below.

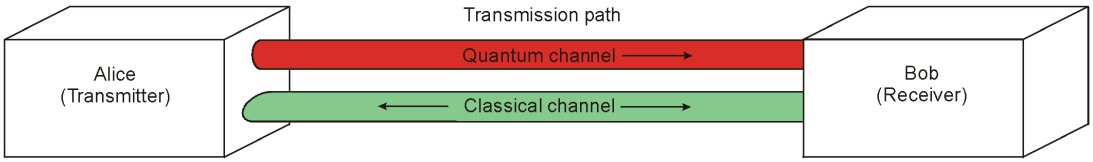


*Figure 3.5. The basic arrangement for QKD between two parties. The transmission path may be free-space, fibre, or even vacuum. The quantum channel is usually one way whilst the classical channel is requires two-way working but is public (meaning open and unencrypted). The classical channel can also be used later for encrypted message transmission.*

The protocol makes use of polarised photons (although BB84 can be implemented in many other ways) to exploit the peculiarities in quantum mechanical measurement to produce secure keys at two locations. The quantum mechanical properties exploited are elements of the Heisenberg uncertainty principle and the quantum no-cloning theorem.

These effects imbue BB84 with certain properties:-

- Measurement of a quantum state in an incorrect way will yield no information on the state being measured.
- Once a state has been measured it will "flip" to the measured state and continue to evolve from that state
- One cannot arbitrarily clone quantum states.

Together these properties enable the key exchange to take place and minimise the amount of information leaked to an eavesdropper. Furthermore, analysis of the quantum bit error rate (QBER) allows the users to detect the possible presence of an eavesdropper on the quantum channel. The QBER of a QKD system is essentially the ratio of erroneous counts to the total number of received counts:

$$QBER = \frac{N_{error}}{N_{error} + N_{correct}} \qquad (3.13)$$

The errors in a free-space QKD system typically arise from two sources. The first source is a base error rate resulting from imperfections in the optics of the system. The second source is detector noise which, again, has two components, detector dark count and background radiation. The QBER of a free-space QKD system can thus be defined as [13]:

$$QBER = k + \frac{2Bt}{\mu T L_g \eta} \qquad (3.14)$$

Where: k is the error rate contribution from the optical system

$B$ is the background count rate per second

$t$ is the width of the detector timing gate

$\mu$ is the average photon number

$T$ is the transmission of the channel

$L_g$ is the geometric loss (due to diffraction and beam spreading)

And $\eta$ is the detector efficiency.

### *3.3.2 Protocol operations*

The essential steps of the BB84 protocol proceed as follows:-

1. Alice generates a string of random bits and uses them to choose one of four possible polarisation states which are divided into two separate non-orthogonal bases as shown below.

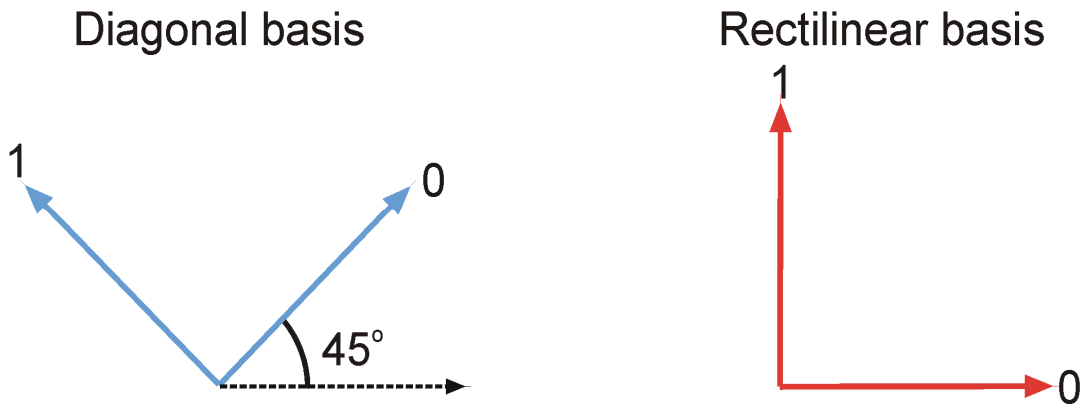


*Figure 3.6. BB84 state preparation. Alice randomly chooses one of four polarisation states, +45$^o$ and-45$^o$, forming the diagonal basis or vertical and horizontal, forming the rectilinear basis.*

2. Alice is careful to keep a complete list of the emission time, photon state and basis which she prepares. The photons are then sent in a string across the quantum channel to Bob as shown in Figure 3.7.

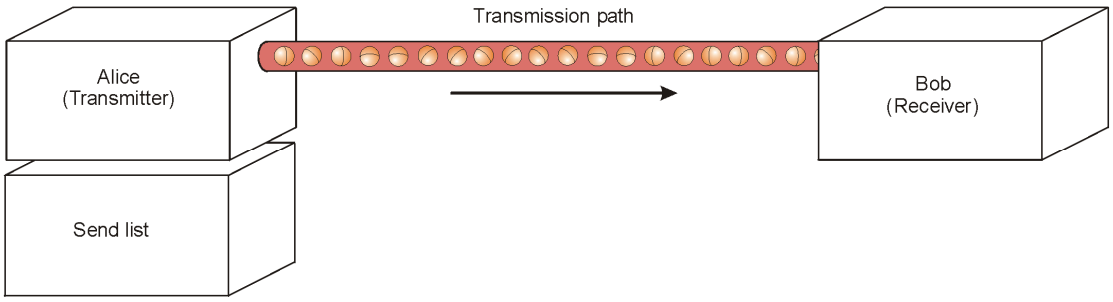


*Figure 3.7. Alice creates a string of polarised photons selected at random from a set of four and sends them to Bob over the quantum channel.*

3. At the other end of the quantum channel, Bob receives a subset of the Alice transmission. There are missing photons due to losses in the channel but Bob faithfully records the time of arrival of all photons he receives and then proceeds to analyse each photon using a random choice of base.

This means that 50% of the time Bob measures in the wrong basis and hence Bob only records meaningful measurements for half of his detected photons.

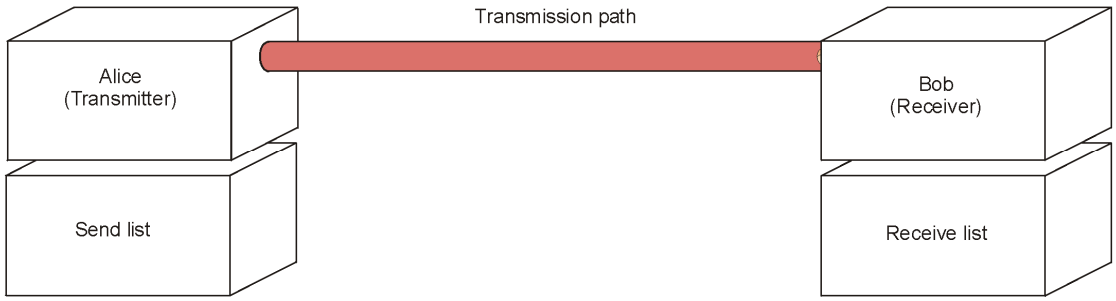


*Figure 3.8. With the quantum transmission complete, Alice and Bob now have a list of photon polarisation states. However, due to losses and noise, the list at Bob is an inaccurate subset of that at Alice.*

4. The situation now is that Alice and Bob each have a list of photon states but the list at Alice is complete whilst the list at Bob is a subset of that at Alice but with errors due to noise, channel losses and possibly even eavesdropper induced errors.

5. The protocol then continues on the public classical channel. Bob sends Alice a list of the times of his successful detections and the basis in which the detection was made (but crucially, not the actual detection value).

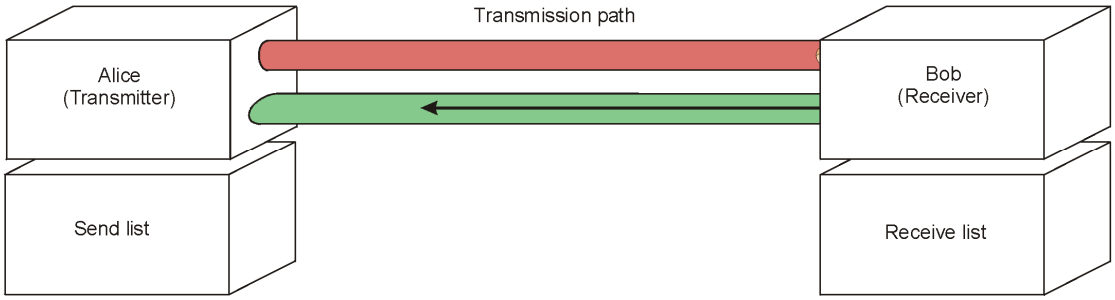


*Figure 3.9. Bob now sends Alice the list of arrival times of the photons and the basis in which he measured each incoming photon. Note that he does not send the actual measured bit value.*

6. Alice can then subtract the time of flight of the photons over the quantum channel and extract the values in her list for which Bob has made the correct basis choice. Alice also informs Bob of which photons he measured in an identical base to that in which the photon was sent. Both parties then discard parts of the list which were either not received or that were incorrectly measured.

7. Alice and Bob now possess nearly identical lists. Errors will arise inevitably due to sources of noise such as the transmission medium, imperfections in the physical apparatus etc.

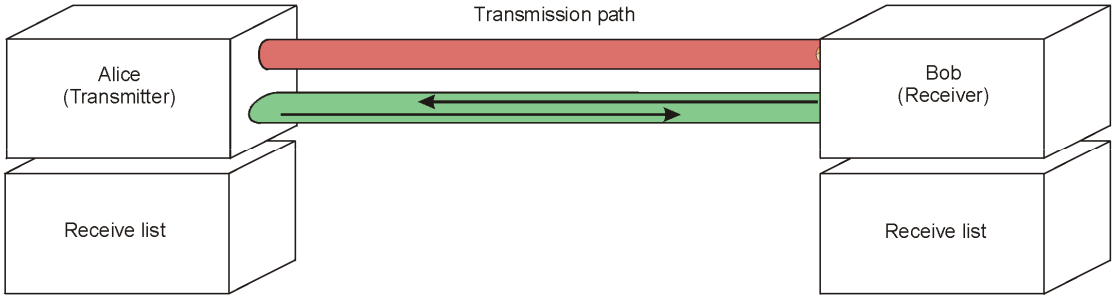


*Figure 3.10. Alice extracts the values from her send list which Bob has told her he received. She then discards all the entries for which Bob made an incorrect choice of bases. She then informs Bob of his correct basis choice measurements. This results in two nearly identical lists at Alice and Bob.*

Furthermore, due to the random selection of outgoing polarisation basis, and since the eavesdropper cannot know in what basis Bob will measure the qubits; any measurement of the photon state will induce errors later on when Bob performs a random measurement of the arriving states. Alice and Bob therefore compare periodically, small portions of key material (which is then discarded), for errors. An elevated error rate at this juncture may indicate an unsound (too noisy) channel or a possible eavesdropper.

Either way the quantum bit error rate (QBER) can give an idea of the most sensible strategy; give up, discard the key and try again, or continue and reconcile the key.

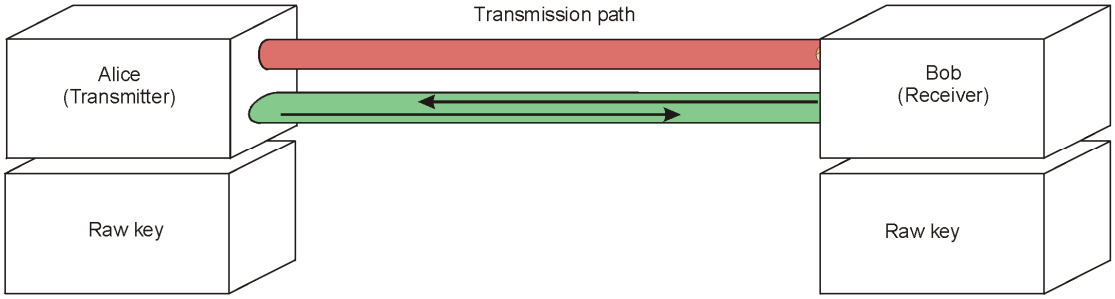


*Figure 3.11. After checking the QBER Alice and Bob both have nearly identical raw keys.*

It should be noted of course that Alice and Bob should have already agreed a secret word with which to authenticate each others identity before commencing the key exchange. For further key exchange sessions, a small portion of the last distilled key can be kept as authentication tokens.

### *3.3.3 Error correction*

In the previous section Alice and Bob were left with two nearly identical key strings and having checked for errors in the keys. Low error rates being indicative of nothing more serious than errors due to noise and physical imperfections in the apparatus.

However, even these small errors can have serious consequences in the encryption and subsequent erroneous decryption of information. For an example of inaccurate decryption see Figure 3.12 below.

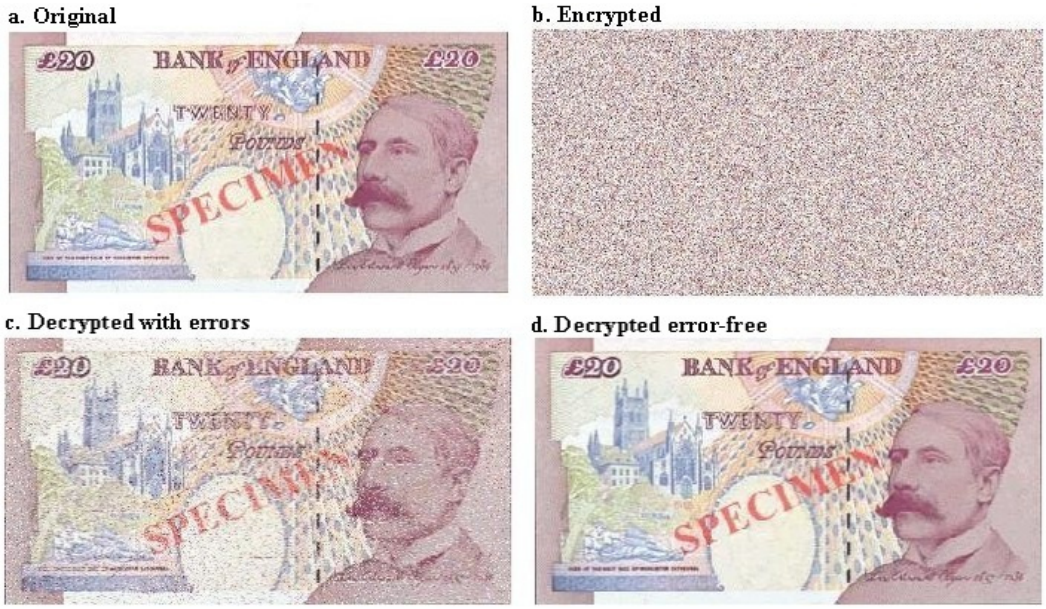


*Figure 3.12. This figure shows inaccurate decryption of a banknote using key generated by a free-space QKD system in 2000 [13].*

With reference to the figure above, **a.** shows a bitmap image of the original banknote. **b.** shows the banknote encrypted with the exchanged key. **c.** shows the imperfect decryption using the uncorrected key, whilst **d.** shows the encrypted banknote decrypted with the error corrected key. The difference between **c.** and **d.** is obvious to the eye but there is clearly much information missing from **c**. Clearly there is a requirement for error correcting the keys resulting from even the most high fidelity key exchanges. This process, usually performed as part of the key exchange process is called error correction.

The information theory of Shannon gives the theoretical minimum amount of public information exchange required to error correct a given message. This quantity of information is described by the Binary entropy function, which can be written thus [14]:

$$f_{er} = -q\log_2(q) - (1-q)\log_2(1-q) \qquad (3.15)$$

Where $q$ is the measured quantum bit error rate of the sifted key.

Shannon, however, does not go on to discuss how one might accomplish the task. However, Brassard and Salvail [15] discuss several error correction codes in their work before settling on a protocol entitled “Cascade” as an efficient method of correcting errors.

Briefly, the Cascade scheme is an iterative process whereby Alice and Bob divide the sifted key into blocks. The parity of each block is then compared across a public channel with those of even parity being accepted as error-free whilst those of odd parity are subjected to further subdivision and comparison until the error is found and corrected. Any errors that occurred in the even parity blocks are detected and corrected by repeating the process several times with different block sizes and permutations. The process continues until Alice and Bob are sure that their sifted keys are identical.

Whilst Brassard and Salvail do not provide a detailed analysis of performance, Tančevski et al [16] provide an estimation of the efficiency of the Cascade algorithm:

$$r_{ec} = \frac{7}{2}q - q\log_2 q \qquad (3.16)$$

Where $q$ is, again, the measured bit error rate of the distilled key.

By way of comparison, equations 3.15 and 3.16 are plotted below in Figure 3.13 with respect to measured bit error rates.

It is clear that whilst the Cascade algorithm by no means approaches the optimum efficiency, it is nonetheless efficient at correcting key strings with error rates of less than 5%.

It should be pointed out that while Cascade is the first and probably the most popular error correction algorithm used in QKD to date, there are several others (for instance low density parity check codes and the Winnow protocol [17]).

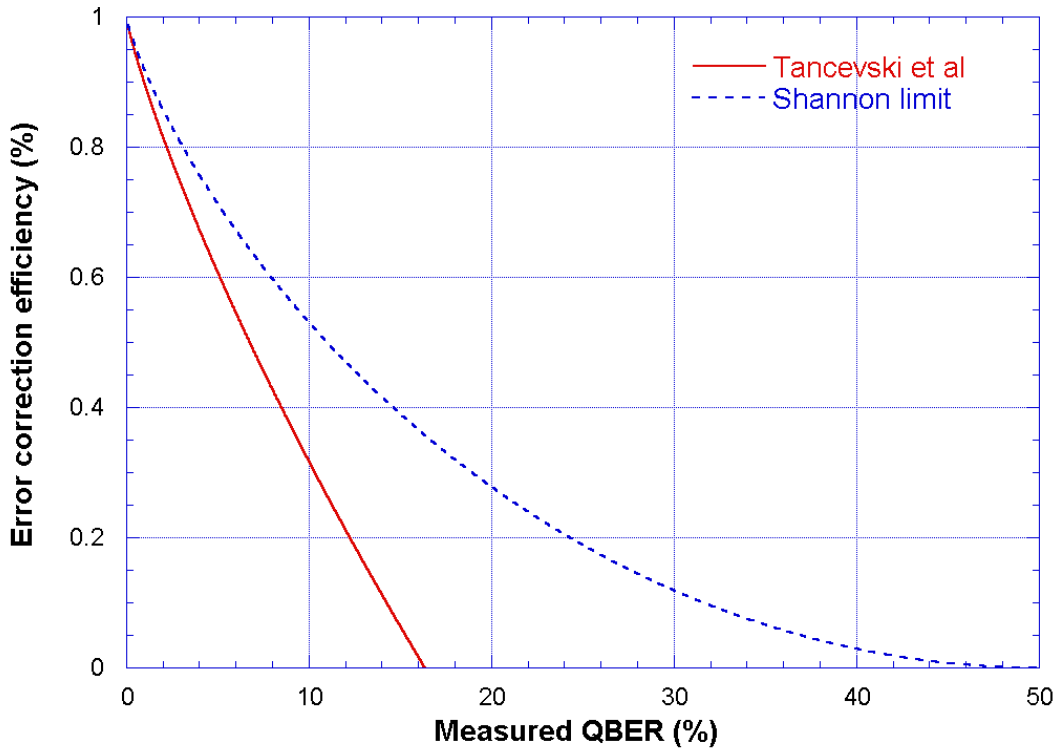


*Figure 3.13. Comparison of Tančevski et al's estimate of the Cascade algorithm error correction efficiency with the theoretical maximum given by Shannon's noisy coding theorem. The estimation gives good agreement for small values of QBER (<5%).*

Much work has been devoted to assessing the relative efficiency of these methods. One thing emerging from this research is that each protocol has its strong and weak points, for instance whilst one protocol may be efficient at error correction, it may require a large classical bandwidth to achieve its efficiency. The converse may be true of another protocol. It is therefore important to select the error correction protocol used with care and reference to available classical bandwidth, predicted error rate and possible eavesdropping strategies.

### *3.3.4 Privacy amplification*

Privacy amplification is the term given to the process of distilling a highly secret key from a partially compromised bit string and is a required further step in the key reconciliation process. This is due to information leakage which occurs as a result of the key exchange and error correction processes.

The amount of information in the possession of an eavesdropper (nicknamed Eve) depends upon factors such as the eavesdropping strategy used, the achieved error rate and the error correction scheme used by Alice and Bob. An example of the "balance of information" in a QKD reconciliation is shown below in Figure 3.14.

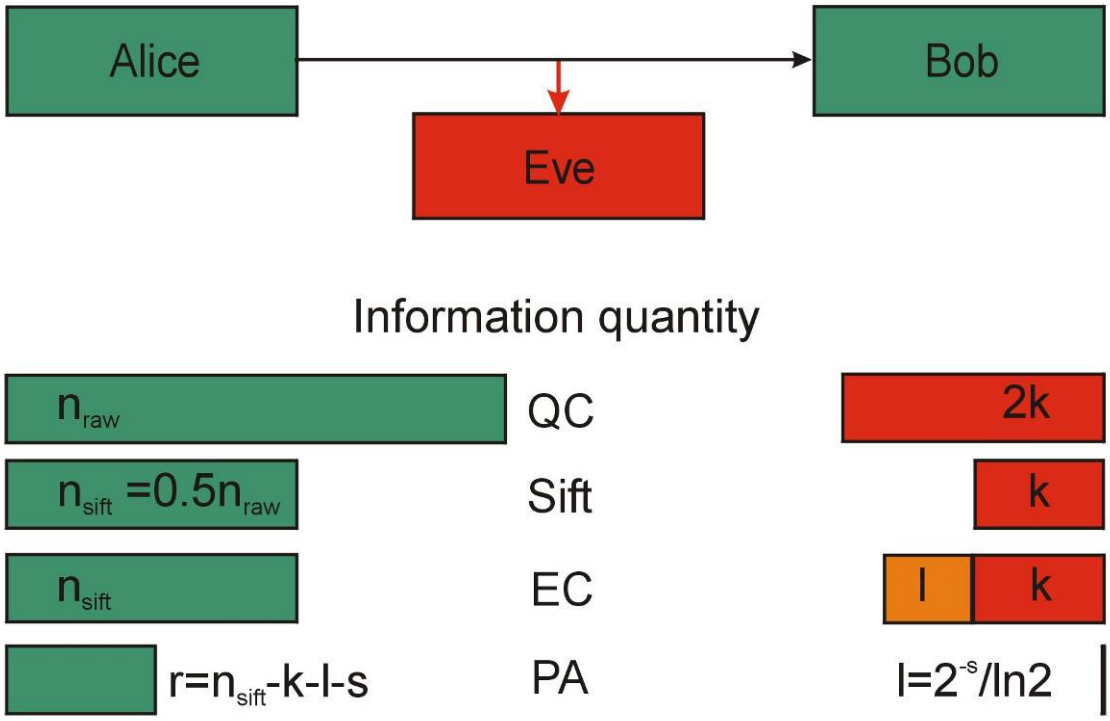


*Figure 3.14 The balance of information in a quantum key exchange as it undergoes key reconciliation. Error correction (EC) corrects errors but leaks information. After privacy amplification (PA) Alice and Bob possess identical secret keys and Eve's information has been reduced to virtually zero (Diagram after [18]).*

Having concluded a successful key exchange, Alice and Bob share an unsifted key, $n_{raw}$. Eve, due to eavesdropping possesses $2k$ information about $n_{raw}$. After key sifting to remove incorrectly measured bases, a shared, sifted key remains, $n_{sift}$. Eve's information is now $k$. Alice and Bob choose an error correcting strategy and proceed to correct their key using public discussion. Eve is able to gain more information from the discussion and now possesses information $k+l$. Alice and Bob use a procedure called universal hashing which can be used to reduce Eves information by reducing their mutual information by a reasonable estimate of the leaked information $k+l$ plus an additional security factor, $s$.

Alice and Bob now possess identical keys $r=n_{sift}-k-l-s$ whilst Eve possesses information $I \leq 2^{-s}/ln2$ [19].

## 3.4 Security of QKD

QKD is often stated to be "unconditionally secure" and from a theoretical standpoint this statement can be shown to be true inasmuch as QKD security is reliant on the validity of physical laws rather than mathematical complexity.

However, given that one is obliged to operate in the real world, compromises must be made from an engineering point of view in order to build working QKD systems. (A good example of this is the use of weak coherent pulses for QKD sources instead of pure single photon sources as described later in section 3.4.2). This gap between theory and practice inevitably creates opportunities for a potential eavesdropper to gain information about the system.

Over the years there has been intense effort devoted by stalwart researchers (such as Lo, Preskill, Mayers, Lutkenhaus, Inamori and others) in developing security proofs for QKD. The field has witnessed significant progress from the ingenious but limited proofs of the early years [20] to more complete treatments which include imperfect sources and detectors [21].

More recently, the idea of "Quantum hacking" has become somewhat more respectable in the community [22] with a combination of acceptance by system builders that attempts to break the security of their systems can provide a degree of awareness of the vulnerabilities of practical implementations and a more responsible attitude from the hackers. This competition between system builders and hackers mimics the wider, age-old conflict between codemakers and codebreakers.

### *3.4.1 The eavesdropping model*

The usual model for security proofs is to limit the sophistication of the QKD system under investigation to current technology whilst allowing the eavesdropper, Eve, access to any (including future) technology, subject only to the laws of physics (For example Eve cannot create clones of unknown quantum states). In this way a security proof can be made valid for any attacks designed in the future. Eve is also allowed to have accomplices to help subvert the system under attack. Alice and Bob are usually assumed to be honest and operate their equipment in secure locations. Another assumption that is usually made is that all errors arising from noise in the system are due to Eve and not to physical imperfections in the apparatuses of Alice and Bob.

There are several ways in which a potential eavesdropper might attempt to gain an advantage by exploiting the implementation of a QKD system or protocol.

These methods can be divided broadly into two classes:

- Attempts where Eve passively steals photons or otherwise manipulates the characteristics of the quantum channel. For instance:
  - Man in the middle (or intercept/resend)
    - Time-shift attack [23]
    - Phase remapping attack [24]
  - Beamsplitting
  - Photon number splitting
- Attempts at eavesdropping where Eve actively manipulates the system or otherwise makes a side channel attack:
  - Breakdown flash of detectors [25]
  - Large pulse attack [26]
  - Dazzle or blinding attack [27], [28]
  - Spectral or spatial eavesdropping
  - EMC or acoustic eavesdropping

Counter measures are available which efficiently deal with those attacks listed above. For instance the photon number splitting attack can be dealt with by using a modified protocol such as the Decoy state protocol proposed by Hwang (discussed later). For the engineering-based attacks such as EMC eavesdropping, the countermeasure is good system design with appropriate screening against emissions. This should also serve to protect against so-called "phreaking" attacks where Eve attempts to subvert Alice or Bob by influencing the apparatus itself.

### *3.4.2 Practical single photon sources.*

Ideally the preferred source for QKD would be a single photon gun, i.e. a source of photons which would provide one, and only one photon, on demand, for every trigger pulse. However, whilst the area of single photon sources is receiving great interest (see [29] & [30] for a couple of good reviews of the subject), there is not, as yet, a conveniently available, reliable, single-photon source for quantum information applications. In spite of this drawback, for practical purposes, it is possible to mimic a single photon source by using "classical" source such as a pulsed laser and strongly attenuating its output such that the average output power is consistent with that of a single photon.

This simple type of source is known as a weak coherent pulsed (WCP) source of photons and since its use by Bennett and coworkers in the first QKD system [31], it has become the source of choice for most non entanglement-based QKD experiments.

Now, whilst WCP sources are very useful in practical systems, they suffer from an important drawback. The pulses emitted by WCP sources exhibit Poissonian statistics. That is, the number of photons in each pulse can be described by a Poissonian distribution such as that shown below in equation 3.17. and plotted in Figure 3.15.

$$P_{\mu}(n) = e^{-\mu}\mu^{n} / n! \qquad (3.17)$$

This means that whilst the average power of the laser may be at the single photon level, the energy in any individual pulse may be consistent with that of two, or even more photons thus rendering a system vulnerable to a so-called photon number splitting attack (PNS attack).

The distribution of energy in a pulse for several output energy settings is shown in Figure 3.15. below. As can be seen from the plot, for a mean photon number (commonly denoted by the symbol, μ) of 0.1, 90% of the pulses will be empty (otherwise known as vacuum pulses), whilst only 8.9% of the pulses will contain a photon. However, there is also a finite probability of multiple photon pulses (0.5% and 0.1% for 2 and 3 photons respectively).

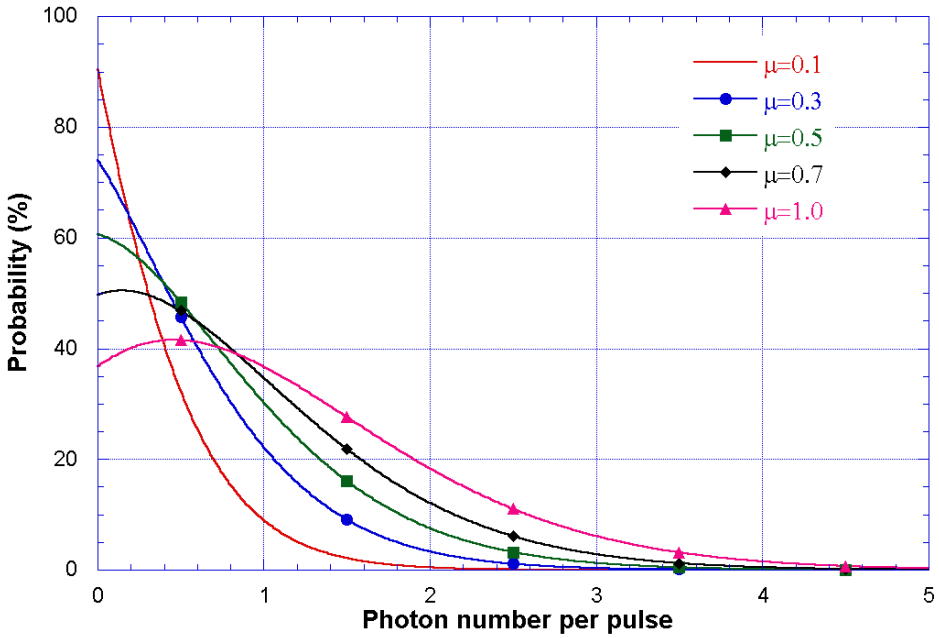


*Figure 3.15. Poissonian distributions for several values of output pulse intensity. One sees, for instance, that for a WCP source with an average photon number, μ, of 0.1 photons per pulse, there is a significant probability that much of the time pulses with 1, 2 and even three photons are emitted resulting in serious consequences for system security.*

By choosing a low average photon number one can limit the possible number of pulses containing multiple photons and thus attempt to mitigate potentially serious consequences from a security point of view. However, as shown above, this choice also limits our bit rate (by an order of magnitude in the case of setting μ at 0.1 photons per pulse) since the vacuum part of the pulse does not contribute (as such, see [32] for an interesting comment on vacuum states) to the final key rate.

### *3.4.3 Why 0.1 photons per pulse?*

Glancing through much of the literature on practical QKD experiments it would be easy to imagine that an average photon number of 0.1 photons per pulse is *de rigueur* in a practical QKD system.

Indeed, the first system built by Bennett and colleagues employed a green LED emitting with a $\mu$ of approximately 0.1 [31]. From then until 2000 nearly every WCP system (for example, Muller et al [33], Townsend et al [34] and Franson & Jacobs [35] to name but a few) employed the same value with little or no proof (although using very reasonable justifications as to the potency of potential eavesdropping technology).

The many security proofs (see, for instance [36], [37] & [38]) that appeared during these early years appeared either to be unaware of the problem or assumed the use of perfect sources (Notwithstanding the technical difficulties in formulating a valid security proof under these circumstances).

The situation was to change in 2000 with the publication by Lütkenhaus of a security proof introducing the idea of a system gain per bit sent value [39]. This concept allowed a rigorous proof of QKD with the not altogether happy outcome that WCP sources may not in fact be very practical for QKD. This proof was further extended over the next couple of years [40] and resulting in a proof [41] of the so-called extended photon number splitting attack and concluding that WCP are not safe for use in real world QKD systems. That is, that weak coherent pulses become unsafe when the application involves long transmission lines, a noisy environment or inefficient detectors. Of course, other opinions differed on the subject, some concluding that for a real world fibre system, for instance, a $\mu$ of 1.1 was sufficient for a realistic system [42]. It should be noted here that there is a big difference between a realistic implementation of QKD with current technologies and an unconditional proof of the security of QKD wherein the potential eavesdroppers can access future technologies.

Much of the discussion was rendered moot, however, in 2003 with the publication by Hwang [43] of a proposal for a modification to the BB84 protocol in the form of the use of decoy state pulses. In short, the QKD transmitter would deliberately introduce multiple photon (or vacuum) pulses into the BB84 transmission phase, effectively intensity modulating the quantum channel. Any interference by an eavesdropper will become apparent later when Alice and Bob perform the reconciliation phase of their protocol. The changes necessary for decoy state operation were cheap and simple to implement (a modification to the Alice hardware and some software tweaks) and allowed systems to operate at higher values of $\mu$, thus increasing bit rates and/or transmission distances. The first demonstration of decoy state was made shortly thereafter by Lo et al using a commercial system manufactured by idQuantique [44]. The results showed that Decoy state was able to improve over the limits shown by Gottesman and colleagues in their comprehensive analysis of BB84 the previous year [21] (shown below in Figure 3.16.).

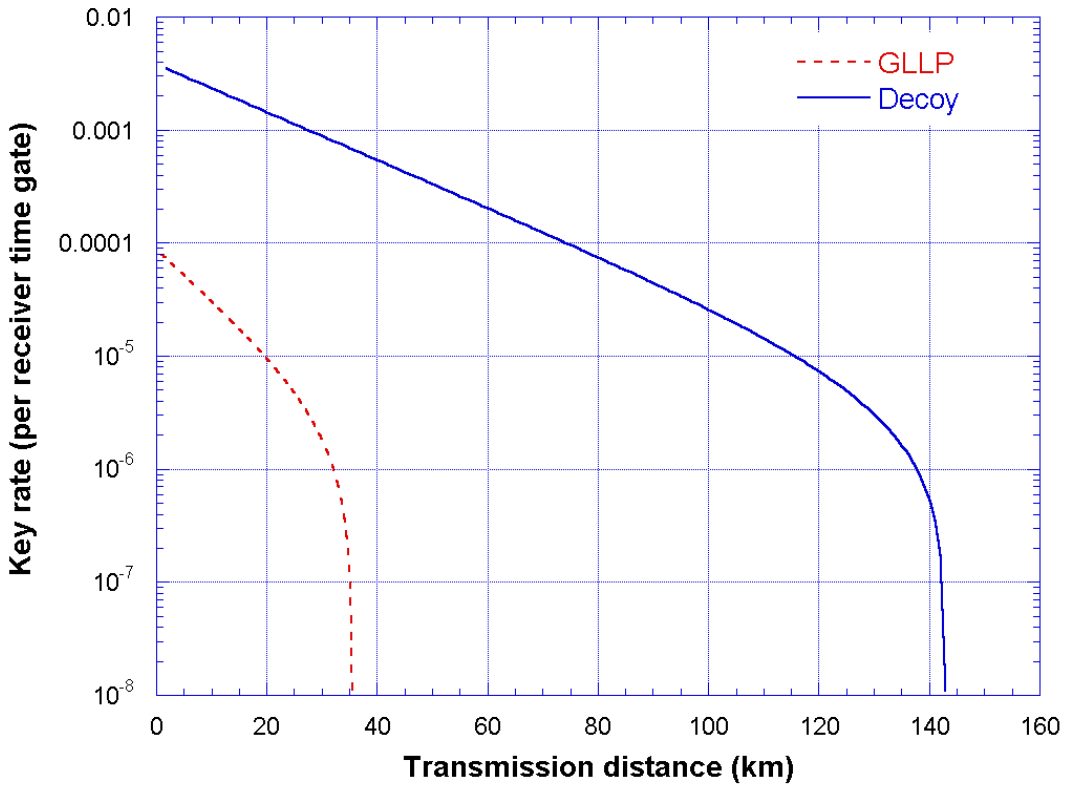


*Figure 3.16. Comparison of performance of BB84 (within the bounds proved by Gottesman, Lo, Lütkenhaus and Preskill [21]) and Decoy state as implemented by Lo et al in [44]. This figure is modelled using the Gobby, Yuan and Shields data used by Lo, Ma and Chen in their 2005 analysis [45].*

Also worth a mention here is the so-called SARG 84 protocol proposed by Scarani et al [46]. By introducing a variation in the classical part of the BB84 protocol it was shown that improved security could result in certain cases.

Although subsequent security analysis by Fung et al [47] showed that broadly speaking BB84 with decoy states generally outperforms SARG84.

So one can see that 0.1 photons per bit was a rather arbitrary, but reasonable, choice for $\mu$, although modern designs of WCP QKD systems tend to employ improved protocols which extend security proofs to more realistic sources as well as allowing larger values of average photon number in the transmission process.

## 3.5 The transmission channel

### *3.5.1 Introduction*

In considering the transmission medium, generally speaking, QKD systems can be divided into two categories, those that use free space and those that use optical fibre. Whilst several QKD system implementations have been tried in both, one media or the other is often intrinsically suited to a particular system implementation. For instance, free-space transmission paths lend themselves to polarisation based systems because free-space is less traumatic to the polarisation state of a single photon than standard optical fibre. For the purposes of this thesis the following is defined:

*Optical fibre*: Any optical waveguide technique for guiding light over long distances (>10m say). For example telecommunications fibre, polarisation-maintaining fibre, plastic optical fibre, etc.

*Free-space*: Any unobstructed line-of-sight optical path between a transmitter and receiver [48] [49]. For example atmospheric transmission and transmission through space but not normally through liquids.

This thesis is primarily concerned with free space transmission but some of the issues associated with fibre transmission will be reviewed.

During the early years of QKD development it was thought that, whilst suitable for proof of principle experiments, free-space QKD was very limited in its application and that for long haul QKD links, optical fibre was the medium of choice for QKD systems.

However, QKD to satellites is mentioned briefly by Franson and Jacobs [50] in their (short range but technically advanced) experiment in 1996 and at least two groups, namely the Hughes team at Los Alamos national labs in the U.S. [51] and the Rarity team at DERA (now QinetiQ) in Malvern U.K. [52] were actively researching satellite-based system feasibility by 2000.

The reason for using satellite technology is that one can distribute secure key material globally using QKD (maybe not the only way? see [53] for some original ideas on the subject). Table 3.1 below summarises transmission medium versus QKD application.

| Application | Optical fibres | Free-space |
|---|---|---|
| Portable | No | Yes |
| Point to point | Yes | Yes |
| Intra-city | Yes | Yes |
| Inter-city | Yes | No |
| Networks | Yes | Limited |
| Last mile | Yes | Yes |
| Global reach | No | Yes |

*Table 3.1. Summary of Transmission medium and general application type.*

It is important to consider all parts of the transmission system when making choices about the transmission channel. For instance, looking at Figure 3.17 below, one might be tempted to operate a QKD system at 1550nm because the technology is mature and there are plenty of commercial off-the-shelf (COTS) components to make life easy. However, since QKD operates in the single photon regime one has to consider detection of single photons, and practically speaking, at this wavelength the choice is limited and, moreover, the available choices are severely restricted in efficiency.

### *3.5.2 Optical fibre transmission media*

Optical fibres span the continents and form the backbone of a global communications network. Communications networks with bandwidths of several TeraHertz are already deployed whilst optical Solitons have been shown to propagate for thousands of kilometres in suitable fibres [54]. It is fair to say, then, that optical fibre based communication systems are a mature technology. This makes the area attractive from the point of view of QKD since there is an extensive amount of infrastructure already in place if one could only make compatible QKD systems. To do this one needs to make a QKD system robust in terms of noise, loss and, in the case of networked fibre systems, security.

#### *3.5.2.1 Loss mechanisms in optical fibres*

It is clear (no pun intended) that glass fibres are a very good transmitter of light. However, there is more to optical fibre transmission than just attenuation.

To make a system work reliably over long distances one has to cope with several fibre properties, including:-

- Attenuation/scattering
- Absorption (material/impurity)

- Dispersion (waveguide/material)
- polarisation related effects
- Birefringence effects
- Other (Mechanical/Thermal/Bending)

This is not exhaustive but extensive nonetheless and all of these properties can degrade signal integrity. Luckily for the designer, not all of these properties have a significant effect on all systems, for instance, many of these effects are negligible for short haul systems, furthermore, some of these properties can often cancel each other out.

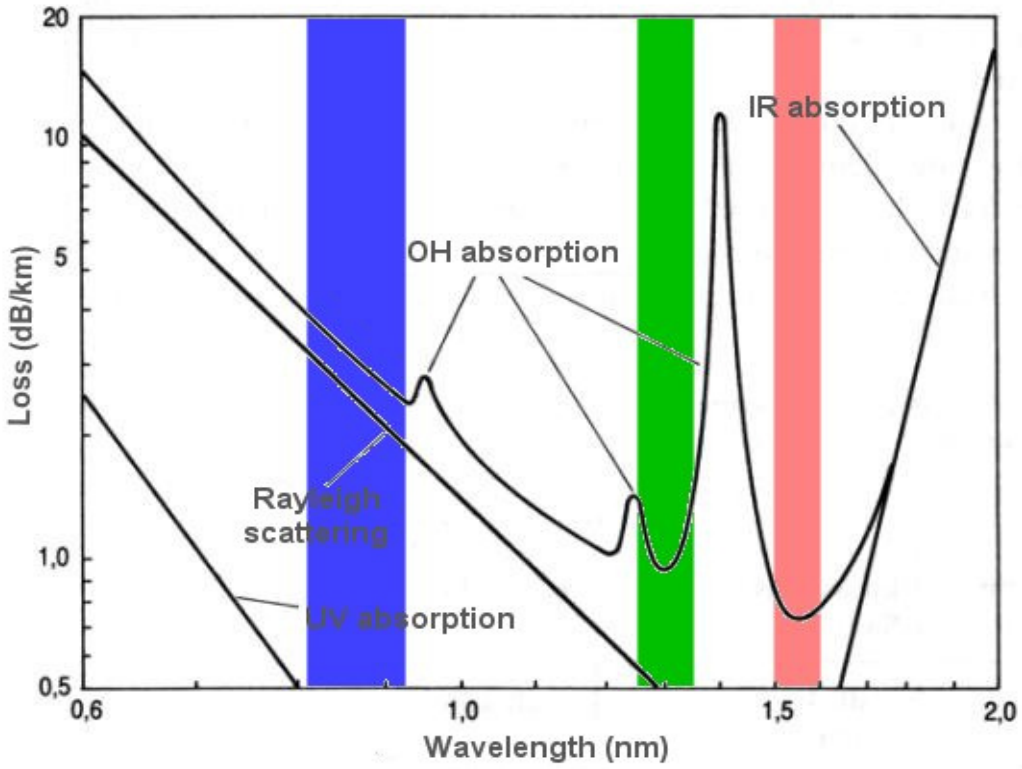


*Figure 3.17. A transmission spectrum of a typical optical fibre showing several of the attenuation mechanisms which contribute to the fibre losses. Also shown are the three so-called telecoms windows at 800-900, 1260-1310 and 1500-1600nm where absorption is at a (local) minimum.*

### *3.5.2.2 Attenuation*

Perhaps the simplest to quantify and the property that places a fundamental limit on transmission distance is signal attenuation in the fibre. Attenuation of an optical fibre is measured in terms of a loss per unit length of fibre and can be best described with the aid of a transmission spectrum like that shown in Figure 3.17.

The transmission curve can be described as the sum of the contributions from all of the effects shown. Additional losses not shown in the diagram may also include coupling losses from fibre joins and bending losses due to manufacturing errors and kinks in the optical cable.

#### *3.5.2.3 Dispersion effects*

Several types of dispersion may occur in optical telecommunications fibre. Types of dispersion encountered may include: Chromatic dispersion (the dependency of the material refractive index to vary with wavelength), Modal dispersion (the tendency of different axial modes to travel at different velocities) and Waveguide dispersion (the dependency of the velocity on waveguide geometry and refractive index profile). The effect of all of them is to broaden or "smear" out optical pulses in time and thus, ultimately, this leads to a limit on the bandwidth of a fibre.

Whilst dispersion can be minimised by the use of narrow channel linewidths (e.g. DWDM systems) and single mode fibres, it is very difficult to eliminate completely and can also be introduced by manufacturing errors and thermal variations. For single photon systems this effectively means that the photon timing jitter becomes broader which can lead to further consequences during the detection process.

#### *3.5.2.4 Birefringence effects*

Birefringence effects occur when an optical material exhibits different refractive indices in different directions within the material. This leads to different propagation velocities through the material for different polarisation components. In practice, although optical fibres are circularly symmetrical and manufactured from fairly homogenous materials, birefringence is always present to some degree due to both thermal and mechanical stresses.

The effect of birefringence can be to "smear" out optical pulses in time as well as actually changing the polarisation state of an optical beam travelling through the birefringent material.

#### *3.5.2.5 Other effects*

All the above effects tend to have strong dependencies on temperature and stress. The effect of this is that not only will the properties of the fibre change due to its environment but they will also change fairly quickly over time, for instance throughout the day whilst the temperature of a cable duct is constantly changing, or even whilst heavy vehicles are passing a cable duct situated by a busy road.

### *3.5.3 Free-space optical transmission*

When considering the atmosphere as an optical channel one often has to take into account the atmospheric path as part of the system since atmospheric phenomena affect the choice of transmitter and receiver hardware and some of the atmospheric effects have a direct bearing on system design (for instance, dealing with the effects of solar background radiation in optical receivers, or pointing and tracking implementation).

Figure 3.18 below illustrates the concept of the system as a whole including the transmission path.

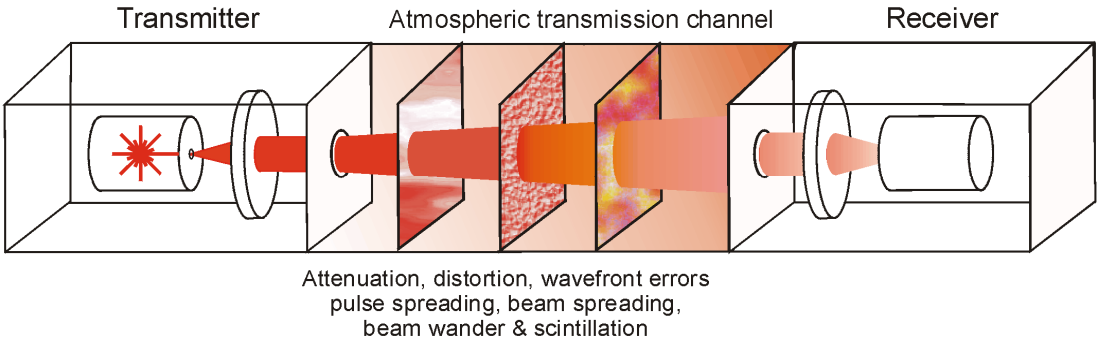


*Figure 3.18. Diagram showing some of the consequences of atmospheric effects on optical transmission.*

Atmospheric phenomena are many and varied and can have a huge affect on the propagation of optical beams through the atmosphere. The main impact of all of these is loss of one sort or another. Shown below is a table listing the main causes of loss in free-space optical transmission systems.

| **Phenomenon** | **Effects** |
|---|---|
| Diffraction | Beam spreading |
| Absorption | Attenuation |
| Scattering | Attenuation, pulse spreading, polarisation distortion |
| Turbulence | Scintillation, signal fading and loss, polarisation distortion, phase distortion |
| Dispersion | Pulse spreading |
| Background radiation | Noise, receiver saturation, damage |

*Table 3.2. Table showing the main atmospheric phenomena and their effects on an optical transmission system.*

Most of these effects depend on a variety of factors such as location, altitude, temperature, season and time of day. With the possible exception of background radiation, all of the effects listed increase with distance and ultimately result in the extinction of the optical beam. For some applications, such as intra-city use, some of the atmospheric effects can be ignored simply because their effects are negligible for short transmission distances. However, as ranges increase beyond a few hundred metres care must be taken to either eliminate or actively compensate for the deleterious effects of these phenomena.

#### *3.5.3.1 Gaussian beam propagation and diffraction*[3]

One of the features of the wave-like properties of light is the property of diffraction. Unlike the situation in optical fibres where the beam of light is in a guided mode, the free-space beam is not so constrained and tends to diffract, or expand, with distance. Such diffraction of the optical beam can be described well if one uses the so-called paraxial approximation, whereby it is assumed that the divergence of the optical beam is small. If the paraxial approximation is valid for a system (and it can be seen later that it is) then one can use the very well formulated Gaussian beam theory for the propagation of the beam.

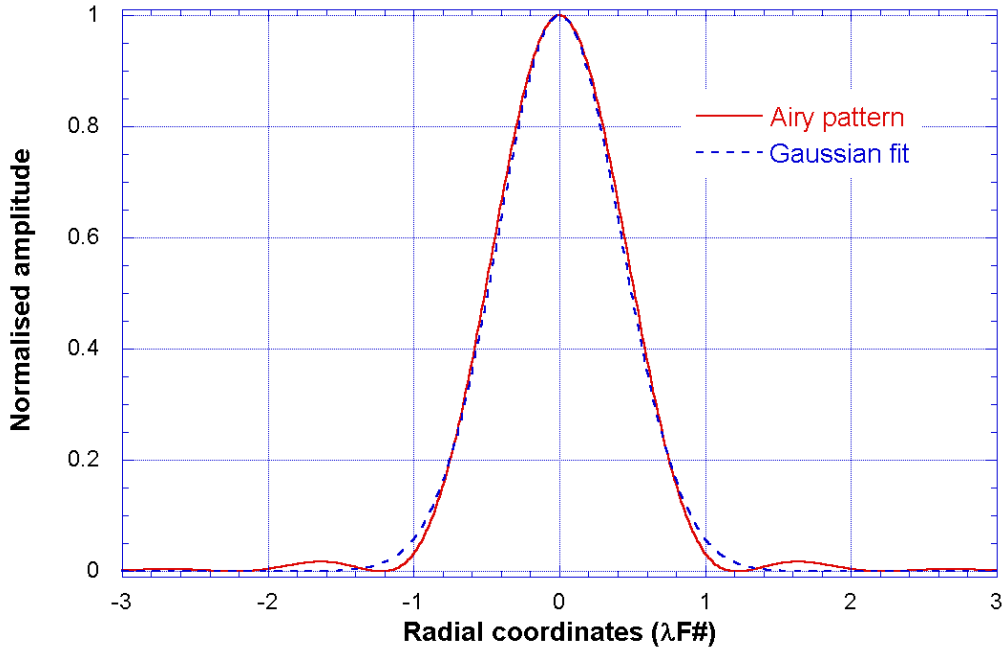


*Figure 3.19. Comparison of the so-called Airy pattern (red) with a Gaussian distribution (blue dotted) of comparable beam width. The two radiation distributions are virtually identical if the subsidiary maxima of the Airy pattern are neglected. Thus a Gaussian approximation is justified.*

[3] This subsection draws heavily on reference [55].

Most WCP QKD systems use commonly available semiconductor laser diodes as sources. Typically, these diodes emit in a well-defined single transverse mode which is also highly astigmatic. There are various methods for circularising the beam (such as Anamorphic prism pairs) but to save space and reduce complexity the required beam shape can be "post selected" by apertures and optics within the transmitter resulting in an Airy type radiation distribution across the beam which can be closely approximated by a Gaussian beamshape. A comparison of the two functions is shown above in Figure 3.19.

For a Gaussian beam of lowest order mode ($TEM_{00}$) and ignoring phase, the amplitude of the field can be written as:-

$$E(x,y,z) = E_0\left(\frac{w_0}{w(z)}e^{-\left(\frac{r}{w}\right)^2}\right) \qquad (3.18)$$

If this equation is plotted a Gaussian distribution is obtained like that shown in Figure 3.20 below.

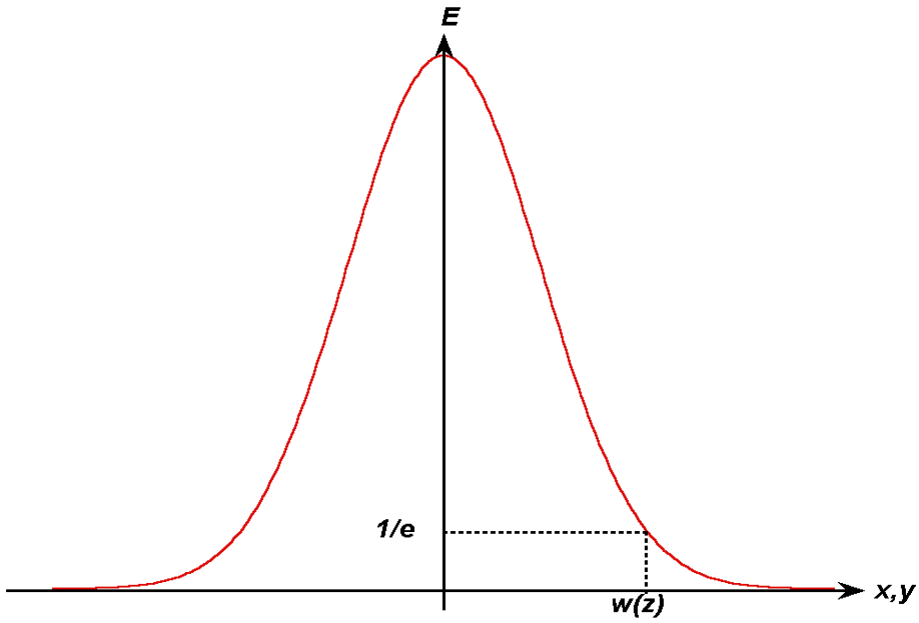


*Figure 3.20. A Gaussian amplitude distribution. The beam waist radius, w(z), corresponds to the point where the field amplitude drops to 1/e of its maximum value. The beam waist radius at its narrowest point is called $w_0$.*

Using the paraxial approximation for a Gaussian beam propagating in the z direction one can write:-

$$\omega(z) = \omega_0\sqrt{1+\left(\frac{z}{z_r}\right)^2} \qquad (3.19)$$

Where $\omega_0$ is the minimum beam radius (often called the beam waist) and $Z_r$ is given by:-

$$z_r = \frac{\pi\omega_0^2}{\lambda} \qquad (3.20)$$

And is often called the Rayleigh range and is the distance from the beam waist to the location where the area of the beam has doubled.

Another definition of the Rayleigh range is that it forms the boundary between the Fresnel and Fraunhofer diffraction regimes.

If the shape of the waist is plotted as the beam propagates in the *z* direction an idea of how the Gaussian beam evolves with distance is obtained. This is shown in Figure 3.21 below.

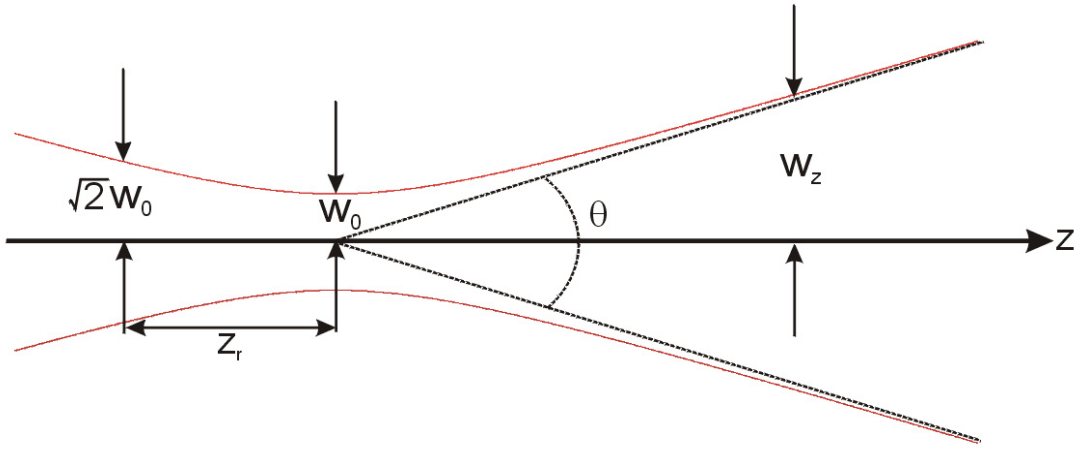


*Figure 3.21. The propagation of a typical Gaussian beam. The beam retains its shape as it propagates but spreads out in the x and y directions. Beam waist, $w_z$ at location z has its minimum value, $w_0$ at $z_0$. (beam waist is usually measured at the $1/e^2$ points of the beam profile). $Z_r$ is called the Rayleigh range or confocal parameter and is the distance over which the beam doubles in size.*

One may also write an expression for the radius of curvature of the resulting wavefronts as:-

$$R(z) = z\left[1+\left(\frac{z_r}{z}\right)^2\right] \qquad (3.21)$$

Examination of the expression above reveals that as $z$ approaches $z_r$, the wavefront radius of curvature increases until at $z=z_0$ it becomes infinite and the wavefront is planar. This is shown below in Figure 3.22.

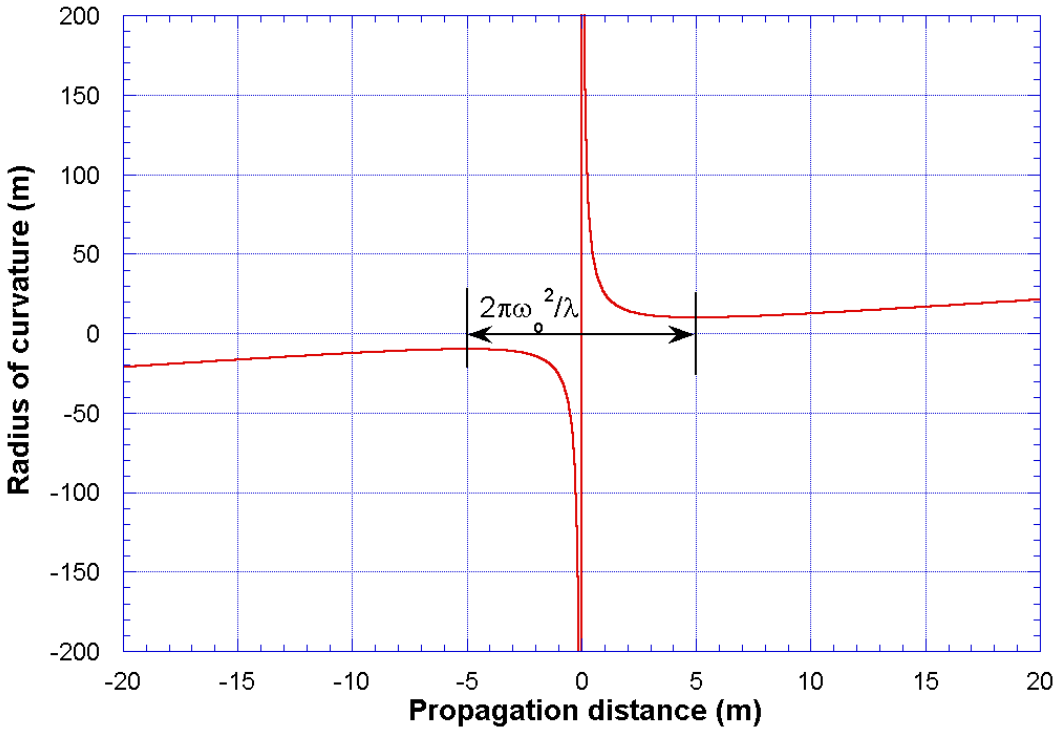


*Figure 3.22. Radius of curvature of the wavefronts for a Gaussian beam propagating from a beam waist of 1mm. Notice how the ROC tends to infinity at the position of the beam waist. Also note how once the beam has left the confocal region (2×Rayleigh range), the ROC increases more or less linearly with distance.*

Another important figure of merit for optical beams is the divergence angle which, from the above, can be defined as:-

$$\theta = \frac{\lambda}{\pi\omega_0} \qquad (3.22)$$

This is the minimum divergence that the beam can have (for the $TEM_{00}$ mode) and, as one can see from Figure 3.21. this equation is only valid when the value of $z >> z_r$, a region which, by definition, is known as the far-field.

This implies that divergence is proportional to wavelength and inversely proportional to the beam waist size.

For single mode beams this allows us to define a quantity called the beamwidth-divergence product which is a constant for a particular Gaussian beam and only varies with wavelength (for example, for a 1μm wavelength beam diverging from a beam waist of 1mm, the BDP is approximately 1.35mm.mRad).

Figure 3.23. below shows how beam diffraction from small apertures can result in unmanageably large beam sizes after propagation over realistic distances.

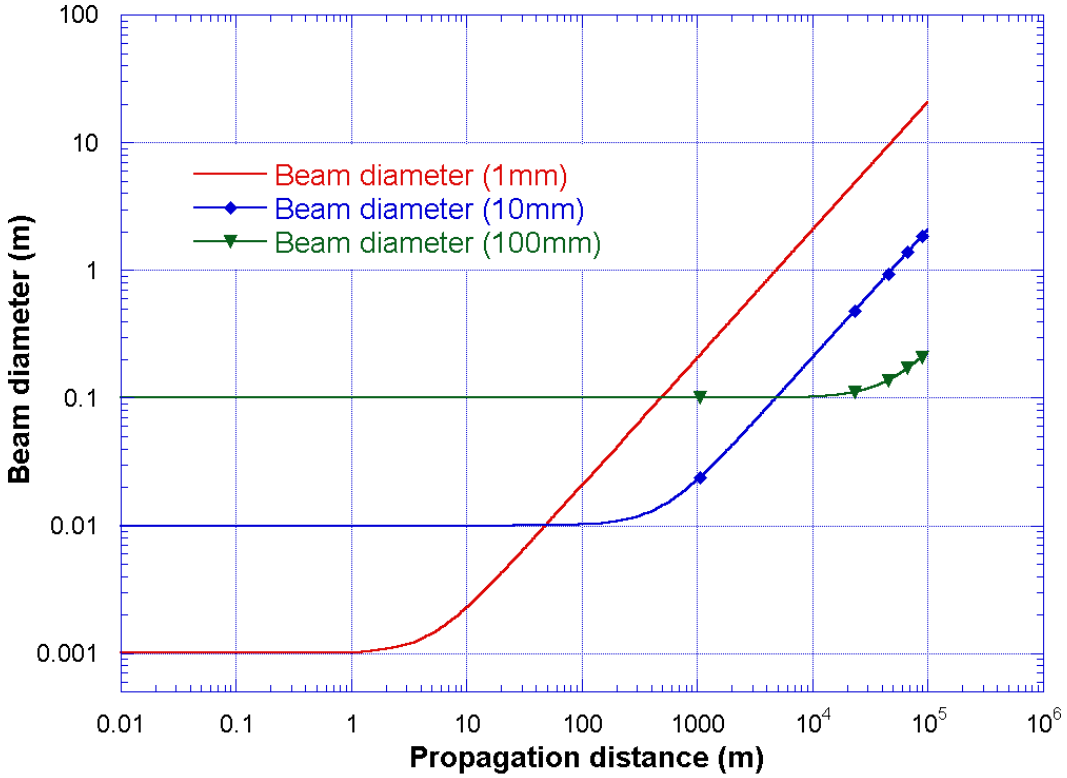


*Figure 3.23. Beam diameter sizes for 650nm wavelength Gaussian beam propagation from different size beam waists. Beams diffracting from small waists can end up unmanageably large over realistic transmission distances.*

The implications for long haul free-space optical systems are obvious. Fortunately the BDP also implies that propagation from larger beam waists or apertures result in smaller beam divergence. This can be achieved by using telescopes at the system output to magnify the beam (which reduces divergence by the same factor).

#### *3.5.3.2 Atmospheric absorption and scattering*

The propagation of an optical beam through any medium other than perfect vacuum will be subject to signal loss or attenuation. This loss is due, in part, to absorption by the atmospheric constituent gases as well as other components such as dust, smoke, aerosols and water vapour. Like any absorption process this will give rise to an absorption spectrum for the transmission medium with features characteristic of the constituents of the actual transmission path.

Another loss mechanism contributing to the signal attenuation is scattering. This can occur from particles of dust and droplets in the atmosphere as well as microscopic density changes in the gases which make up the atmosphere. Scattering phenomena have different effects at different wavelengths depending on the nature of the scattering species.

The two main scattering mechanisms of interest are:-

- Rayleigh scattering – scattering due to objects much smaller than the wavelength of the light such as atoms and molecules.
- Mie (or aerosol) scattering - scattering due to objects larger than the wavelength such as aerosols and particulates.

Both effects are considered to be elastic scattering processes whereby the energy (and therefore the wavelength) of the light remains unchanged. In addition, both are wavelength and particle size dependent with Mie scattering also depending strongly on the type and shape of scattering agent.

The resultant attenuation due to scattering and absorption is often expressed as a simple expression analogous to that of the attenuation length in optical fibres. This is known as the Beer-Lambert law and can be written thus:-

$$T = e^{-\gamma R} \qquad (3.23)$$

Where $T$ is the transmission

$R$ is the range

$\gamma$ is a coefficient which is usually expressed as a sum of several contributions from different scattering and absorption species such as molecular and aerosol absorption.

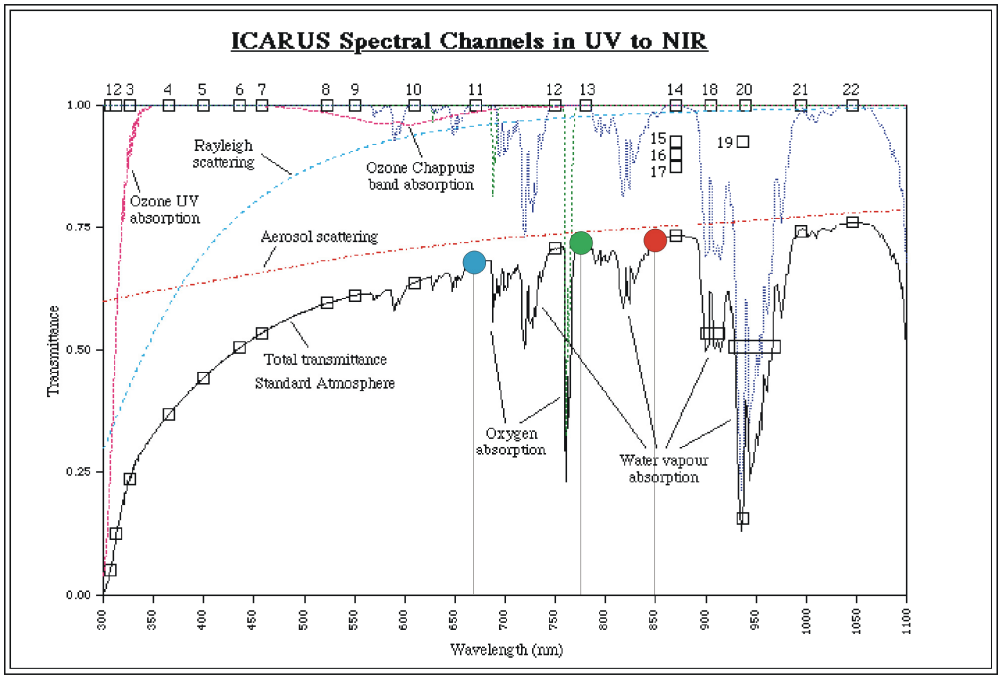


*Figure 3.24. The ubiquitous NERC/RSADU plot of atmospheric transmission in the visible and near infra red band showing several important contributions to atmospheric extinction. The plot shows transmission over one air mass (ground to space vertical transmission path).*

The Beer-Lambert law has its limitations and should be treated with caution. For instance the simple form does not allow for changes in concentration of absorbers or scatterers along the transmission path or with time. Furthermore the law breaks down under large concentrations of absorbers or scatterers.

The graph above shows the typical attenuation of the atmosphere for one air mass (a vertical transmission path from the ground to space). Also shown on the plot are three coloured dots signifying the wavelengths used by three different teams in free-space QKD experiments (Blue-670nm Rarity et al, Malvern, U.K., Green-773nm Hughes et al, Los Alamos, U.S. and red-850nm Weinfurter et al, Munich, BRD). The main thing to note is that all three have been chosen for the relatively good atmospheric transmission. Although transmission efficiency is extremely important, there are other criteria for choosing a wavelength of operation and this is the reason why a different wavelength was chosen by each team.

In addition to direct measurements of the atmospheric properties, some accurate models have been constructed which allow realistic modelling of transmission paths with respect to absorption and scattering. LOWTRAN, MODTRAN and Fascode are just three of the many models available for transmission purposes. A typical plot from a MODTRAN simulation is shown below for several realistic experimental ranges.

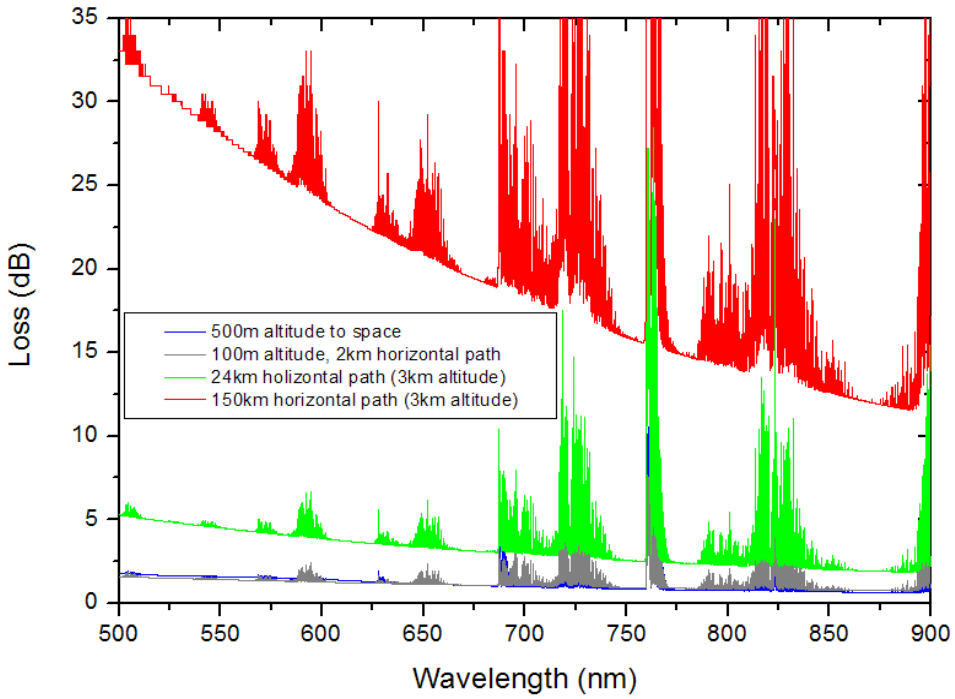


*Figure 3.25. A MODTRAN simulation of four transmission paths through the atmosphere. Note absorption due to molecular and atomic constituents is superimposed onto other losses, which increase at shorter wavelength (mainly due to Rayleigh scattering).*

### *3.5.4 Atmospheric turbulence*[4]

Turbulence is a much studied atmospheric phenomenon which can have a significant impact on free-space optical systems and is caused by small refractive index changes over space and time. These, in turn, are caused by small changes in temperature which result from turbulent motion induced by winds and convection.

Historically, an approach has been taken to describe the atmosphere in terms of a viscous fluid. Such a fluid generally has two distinct states of motion, laminar and turbulent flow.

In laminar flow situations the air moves in layers with little mixing between layers and consequently a low level of energy transfer. Conversely, turbulent flow is characterised by non-uniform behaviour with random eddies leading to mixing between layers and an increased level of heat transfer.

The type of flow exhibited by a viscous fluid is often characterised by a dimensionless number called the Reynolds number (*Re*). For small values of *Re*, the flow is said to be laminar but as Re surpasses some critical value (determined by several factors such as viscosity and density) the flow transitions to turbulent whereupon eddies develop, causing mixing amongst the different (formerly laminar) layers. This turbulent mixing also results in the mixing of other properties of the fluid.

Turbulent motion of a fluid is basically a non-linear process which can be described using the Navier-Stokes equations.

Due to the difficulty in obtaining solutions to these equations, even under favourable conditions, a statistical method of modelling atmospheric turbulence was proposed, initially by Kolmogorov in 1941, by making hypotheses heavily relying on physical insight. Therefore, it should be noted that turbulence theory is not derived from first principles.

Kolmogorov's method made use of an idea first expounded by L. F. Richardson [56] (paraphrasing Jonathan Swift):-

> *"Big whirls have little whorls that feed on their velocity,*
> *and little whorls have lesser whorls and so on to viscosity*
> *—in the molecular sense."*

[4] This section relies heavily upon references [57], [60] and [64]

### *3.5.4.1 Kolmogorov's theory of turbulence*

In Kolmogorov's theory [58], this idea is termed the cascade theory of turbulence whereby the wind velocity increases until the critical value, *Rc*, is reached and turbulent flow ensues consisting of large unstable air masses (eddies) which are smaller than, and independent of, the parent flow. The large (macroscale) eddies break up to form smaller ones, which, in turn, break up to form even smaller eddies and so on until a microscale eddy size is reached and energy is further dissipated as heat. This idea is shown below in below Figure 3.26.

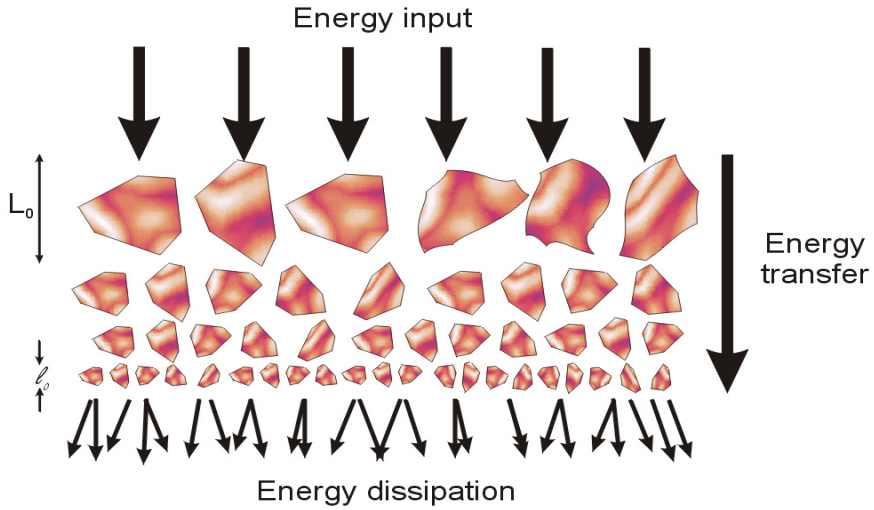


*Figure 3.26. A diagram showing the Kolmogorov cascade theory. Turbules range in size from outer scale ($L_0$) of the order of metres to inner scale ($l_0$) of the order of millimetres, with the difference being termed the inertial range (Diagram after Andrews and Phillips [60]).*

Using this model enables turbulence within this range to be treated statistically under the assumption that the flow is both isotropic and homogenous.

The resulting analysis leads to the definition of a statistical measure called the refractive index structure function $D_n$ such that:-

$$D_n = \left\langle [n(A,t) - n(B,t)]^2 \right\rangle \qquad (3.24)$$

Where A and B are the refractive indices at some point local to each other at time t. The refractive index structure is in relation to the distance between A and B according to Kolmogorov so that:-

$$Dn = \begin{cases} C_n^2 l_0^{\frac{4}{3}} r^2 & \text{for } l_0 << r << L_0 \\ C_n^2 r^{\frac{2}{3}} & \text{for } r << l_0 \end{cases} \qquad (3.25)$$

Where $C_n^2$ is the refractive index structure parameter (in $m^{-2/3}$) and $l_0$ and $L_0$ are the inner and outer scales of the turbule sizes measured in metres. The value of $C_n^2$ varies depending on several factors such as temperature and altitude and takes typical values of $\sim 10^{-16}$ for weak turbulence to $10^{-13}$ for strong turbulence. The value of $C_n^2$ is generally assumed to be a "constant" for a given horizontal transmission path, at least over short time scales, however, given that the atmosphere is generally stratified (on a larger scale than the Kolmogorov scales) the quantity can not be considered constant for vertical or slant paths through the atmosphere of the type that might be encountered by communications systems attempting to communicate with satellites or aircraft at altitude. For these cases other models have been developed.

For the rest of this review of beam propagation under the influence of turbulence the methods described invariably use the so-called Rytov method to analyse atmospheric effects on the transmission of optical beams. The Rytov method (Rytov approximation or method of smooth perturbations) was developed by Rytov in 1937, for the analysis of light scattering by sound waves, and later applied by Obukhov to the propagation of electro-magnetic waves in random media. The method is useful in analysing line of sight optical paths in weak turbulence and includes of diffraction and phase effects [63]. Beam profiles are all typically Gaussian shaped as described above in section 3.5.3.1 above.

### *3.5.5 Beam effects*

Atmospheric turbulence is encountered to some degree when propagating optical (or for that matter, any electro-magnetic) energy along any atmospheric transmission path. The phenomena engendered by turbulence can have significant consequences for optical communications systems and can include:-

- Beam spreading (in addition to diffraction) and beam wander
- Intensity fluctuations (scintillation)
- Angle of arrival fluctuations (image "boil" or "dancing")

These effects can combine to produce severe reduction in received power and distortion in imaging systems. For short range systems these effects do not pose significant problems, however, for systems operating over distances of greater than a few hundred metres, significant beam degradation can occur and remedial measures must be applied to restore efficient system operation.

### *3.5.6 Beam spreading and wander*

When propagating an optical beam through the atmosphere over significant distances the beam spot at the receiver tends to exhibit a random walk due to the beam encountering turbulence induced changes in refractive index along its path. These changes have differing effects depending on their size relative to the beam. For small scale *turbule* sizes the beam will experience some broadening whilst for larger scale *turbules* the beam centroid will be caused to move about randomly as the turbules move across the beam path. In other words the beam is randomly deflected. The situation is shown below in Figure 3.27.

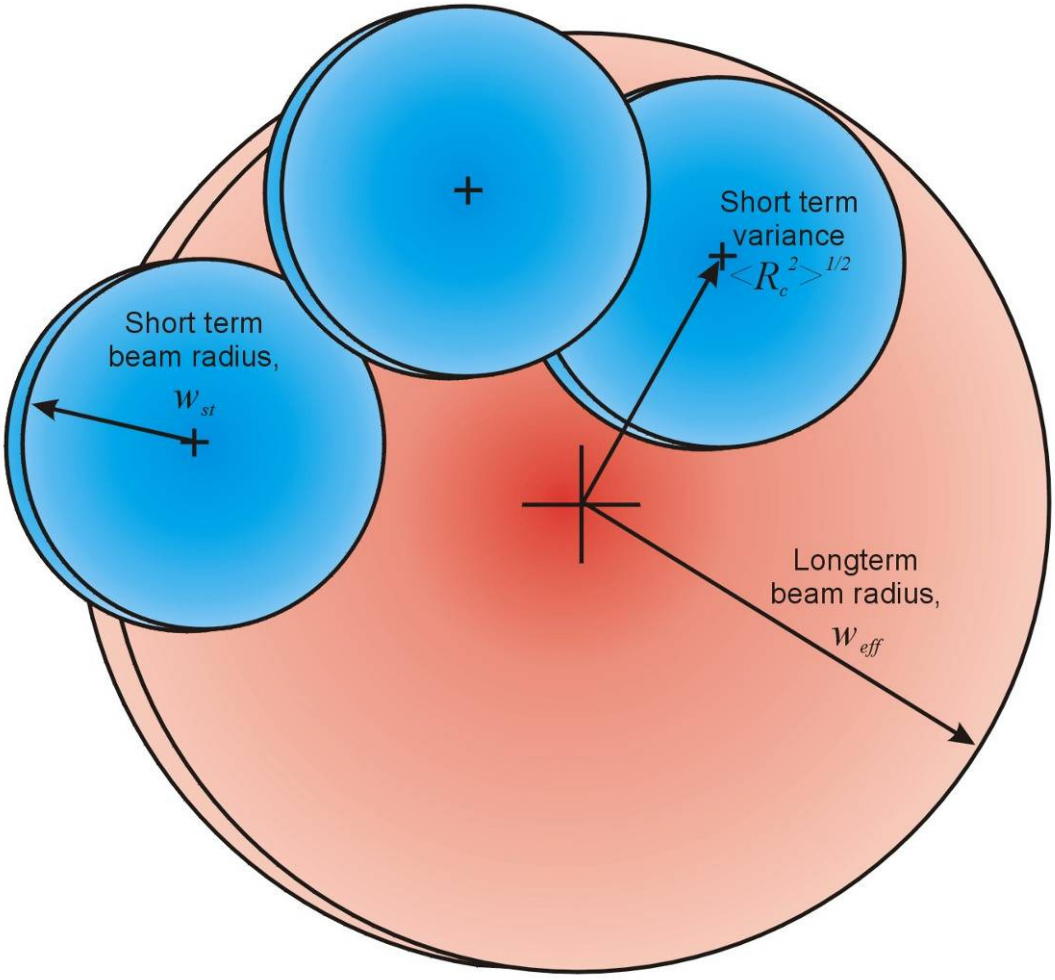


*Figure 3.27. Short term and long term beam radii. The short term radius, $w_{st}$, due to beam spreading will randomly wander over an effective long term radius, $w_{eff}$ (diagram after [60]).*

Experiments have shown that beam wander takes place over time scales of the order of:

$$t \approx \frac{beamsize}{windspeed} \qquad (3.26)$$

So, a short exposure photograph of the beam at the receiver would show a broadened beam ($w_{st}$) offset from the beam axis by some random value. A short time later one would expect to see the same size beam offset by some random, but different value and so on. A photograph of the same scene taken with a much longer exposure would see a much bigger apparent beamsize ($w_{eff}$), with a Gaussian profile with some effective beam size characteristic of the average variance of the beam centroid:-

$$w_{eff}^2 = w_{st}^2 + \left\langle r_c^2 \right\rangle \qquad (3.27)$$

Where $\left\langle r_c^2 \right\rangle$ is the variance of the short term beam centroid described by:-

$$\left\langle r_c^2 \right\rangle = 2.87 C_n^2 L^3 w_0^{-\frac{1}{3}} \qquad (3.28)$$

Using [64] the effective long term beam radius, $\rho_L$ can be written as a beam with an effective radius:-

$$w_{eff}^2 = \frac{4z^2}{k^2 D^2} + \frac{D^2}{4}\left(1 - \frac{z}{F}\right)^2 + \frac{4z^2}{k^2 \rho_o^2} \qquad (3.29)$$

Where: $z$ is the propagation distance

$k$ is the wavevector ($2\pi/\lambda$)

$D$ is the transmitter aperture diameter

$F$ is the initial radius of curvature of the wavefront

And $\rho_0$ is the spatial coherence radius given by:-

$$\rho_0 = \rho_{sp} = \left[0.55 k^2 z C_n^2\right]^{-\frac{3}{5}} \qquad (3.30)$$

Where $\rho_0$ lies within the inertial range, i.e. $\lambda_0 << \rho_0 << L_0$.

An expression for the short term beam radius may now be found using equations 3.27 and 3.28 so that:-

$$w_{st}^2 \approx \frac{4z^2}{k^2 D^2} + \frac{D^2}{4}\left(1 - \frac{z}{F}\right)^2 + \frac{4z^2}{k^2 \rho_0^2}\left[1 - 0.62\left(\frac{\rho_0}{D}\right)^{\frac{1}{3}}\right]^{\frac{6}{5}} \qquad (3.31)$$

A comparison of estimated beam sizes is shown below in Figure 3.28 for diffractive versus turbulence effects.

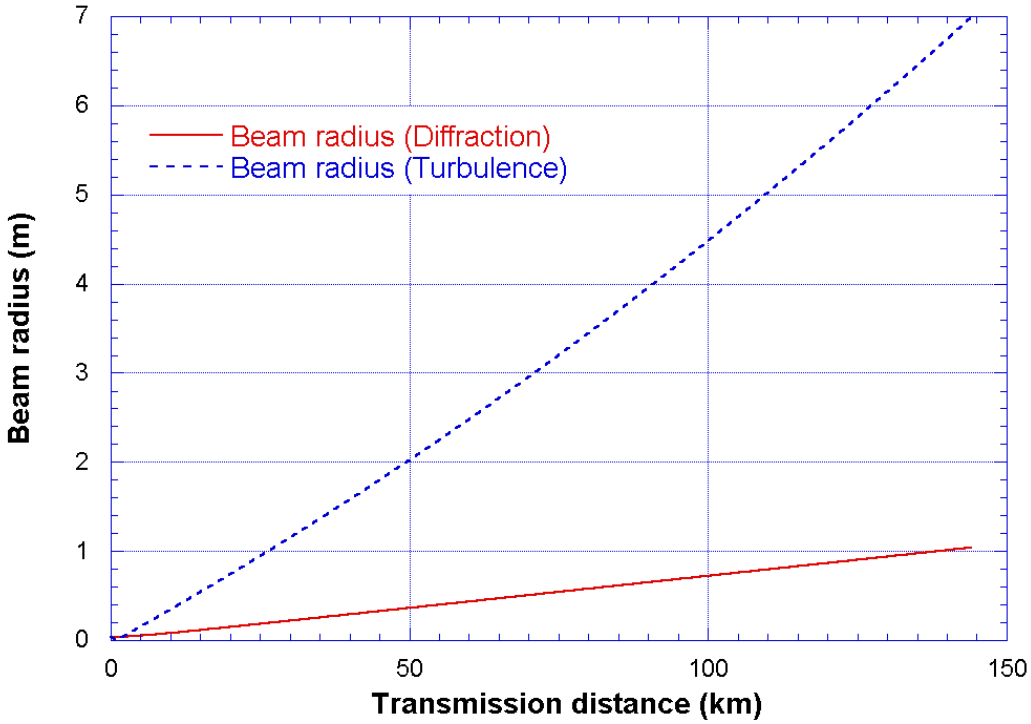


*Figure 3.28. A comparison of beam radii due to diffraction and turbulence using the model outlined above and realistic parameters. Turbulence can lead to large increases in beam diameter at the receiver. The actual results agree well with those reported by T. Schmidt-Manderbach et al during the Tenerife-La Palma experiment [61].*

The effects described above are graphically illustrated below in Figure 3.29. where a single short term exposure is compared with an average of 40 such exposures. Practically speaking beam wander will tend to cause signal fading and dropouts on the timescale of Equation 3.24. Unfortunately, what would be signal fading in a normal communication system, turns into signal loss in the quantum channel.

A way of overcoming beam wander for short range systems is to slightly defocus the beam (or rely on diffraction and beam spreading) in order to contrive to have a beam diameter similar to the value of $\langle r_c^2 \rangle$ such that some of the beam always overlaps the receiver aperture.

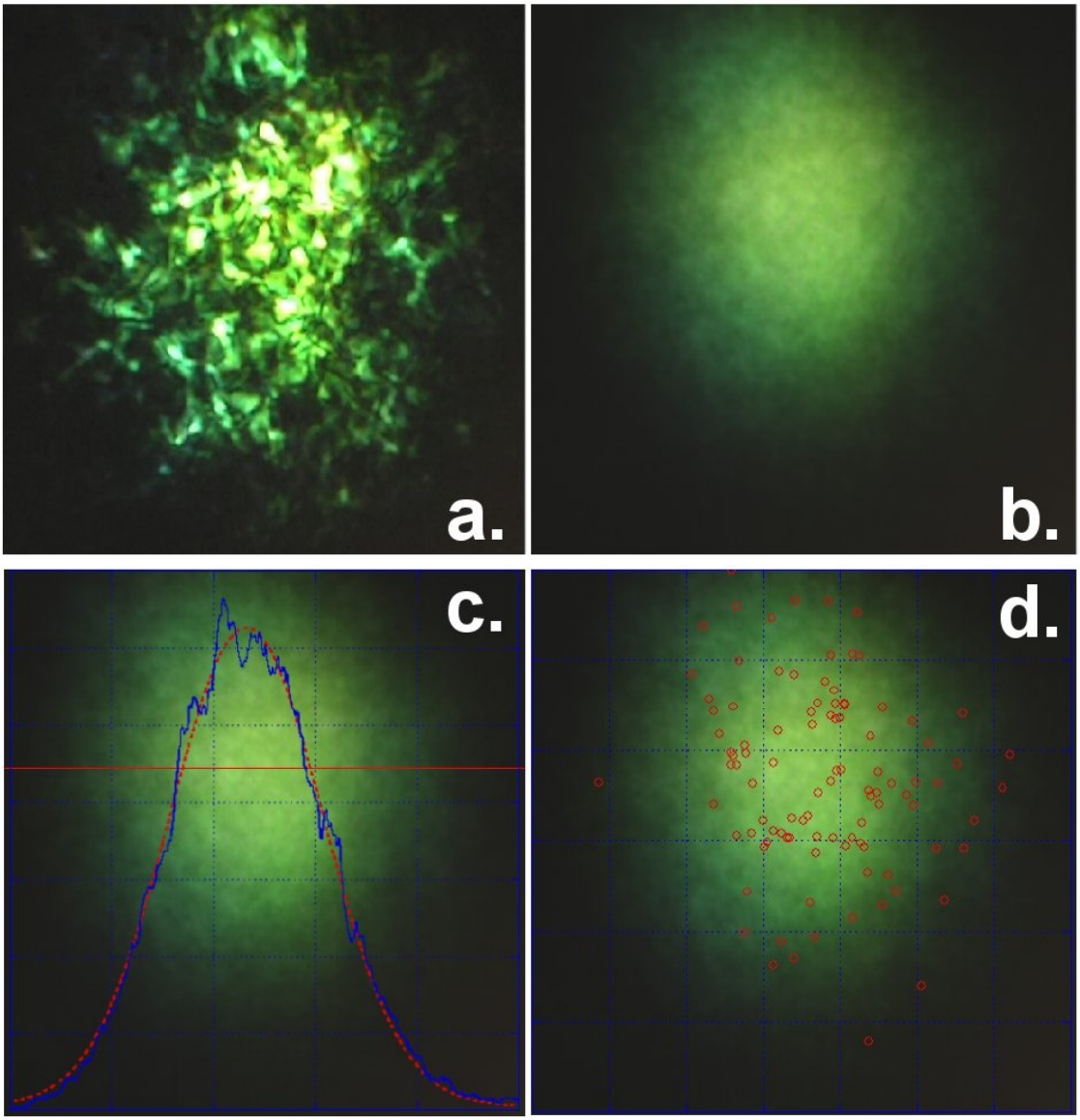


*Figure 3.29. Short term beam compared with a long term averaged beam. a. shows the short term beam structure (including scintillation effects) and size. b. Shows the average of forty such images taken over several seconds. c. Shows the weighted (to account for the fact the image is in colour) profile through b, illustrating the long term Gaussian beam profile and d. shows the location of each beam centroid.(Image processing by A. J. Turner of QinetiQ, Malvern).*

For longer range systems, since the beam wander takes place over relatively long time scales the variation can be compensated by actively tracking the transmitter and receiver. Of course with a QKD system this is difficult since the low fluence makes acquiring the beam extremely difficult using conventional detectors. Another way of tracking is to provide beacons at each end of the transmission path, or, if an optical classical channel is available, this can be used as a tracking aid.

#### *3.5.6.1 Scintillation*

Scintillation is the name given to the effects in the atmosphere which lead to the phenomenon of star “twinkle”. The effect is caused by refractive index changes in the transmission path leading to phase changes across the beam causing both constructive and destructive interference within the beam. This, in turn, causes both spatial and temporal variations in the irradiance of the incoming beam. An example of scintillation is shown below for a collimated laser beam traversing a beam path of 1.2km close to the ground.

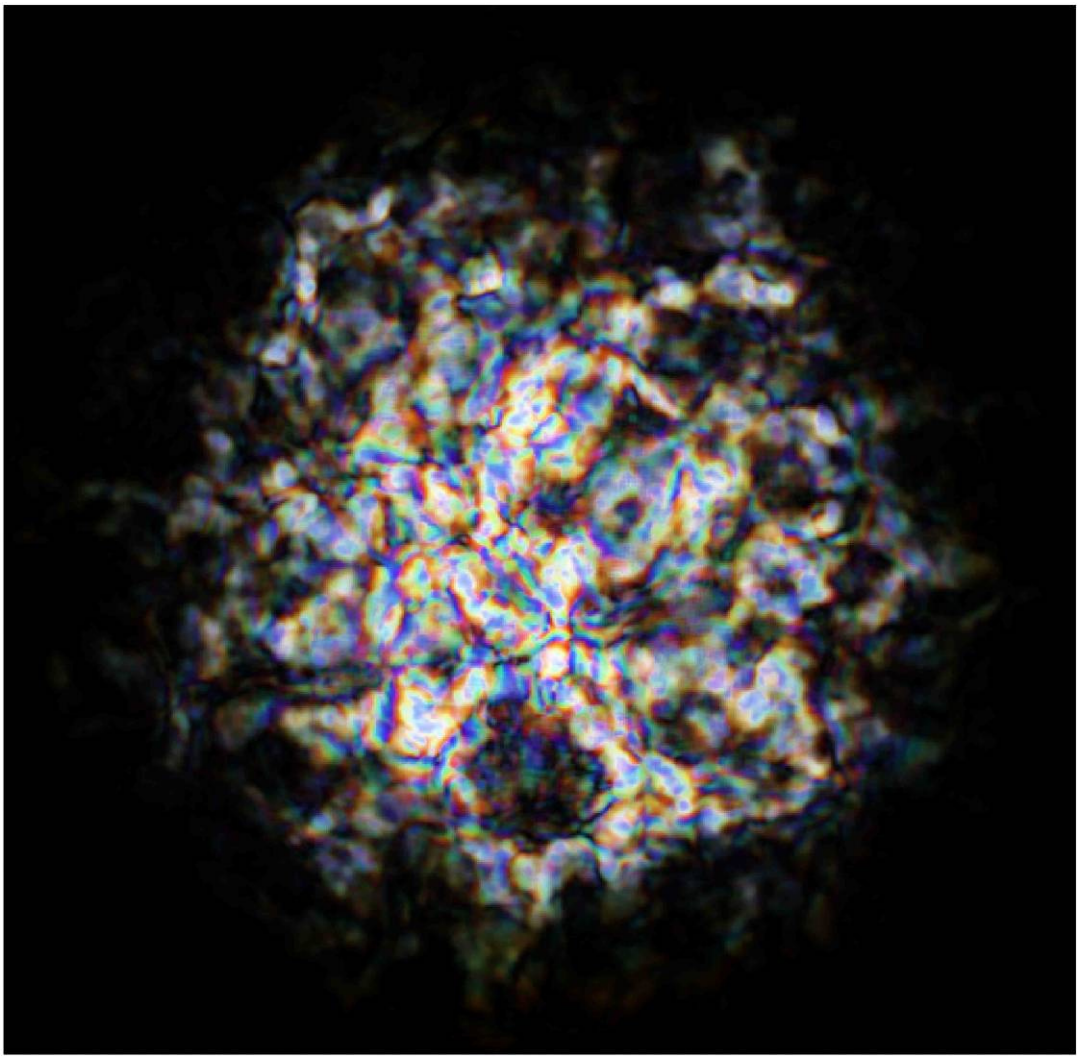

*Figure 3.30. Photograph of a white-light laser beam after traversing a 1.2km horizontal path close to the ground. Examination of the photograph reveals the variation in structure and intensity across the beam. Some atmospheric chromatic aberration effects (blue and red fringes) may also be seen in the structure. Photograph was taken at 1/30th of a second exposure. (Photograph courtesy of Dr. D. A. Orchard, QinetiQ, Malvern).*

In general, atmospheric scintillation effects are characterised by measuring the variance of the amplitude or irradiance at a point in the beam. This leads to a quantity derived from analysis of the fourth order statistics of the propagating beam and known as the scintillation index:-

$$\sigma_I^2 = \frac{\langle I^2 \rangle}{\langle I \rangle^2} - 1 \qquad (3.32)$$

The average size of the variations in intensity or "speckles" can also be characterised by a quantity known as the intensity correlation length, $\rho_0$, which under the weak turbulence regime is of the order of the first Fresnel zone:

$$\rho_0 \approx \sqrt{\frac{L}{k}} \qquad (3.33)$$

Where: $L$ is the path length and $k$ is the wavenumber.

In weak turbulence regimes, the scintillation index is generally accepted to vary in proportion to the Rytov variance [62], which is itself representative of the scintillation index for a plane wave in weak homogeneous turbulence:-

$$\sigma_1^2 = 1.23 C_n^2 k^{\frac{7}{6}} L^{\frac{11}{6}} \qquad (3.34)$$

Where: $C_n^2$ is the refractive index structure parameter

$k$ is the wavenumber and $L$ is the path length.

The Rytov variance is also considered to be a measure of turbulence strength when extended to strong turbulence by increases in path length or refractive index structure parameter. The scintillation index for a plane wave, in the absence of inner scale effects can be written:-

$$\sigma_I^2 = \exp\left[ \frac{0.54\sigma_1^2}{\left(1 + 1.22\sigma_1^{\frac{12}{5}}\right)^{\frac{7}{6}}} + \frac{0.509\sigma_1^2}{\left(1 + 0.69\sigma_1^{\frac{12}{5}}\right)^{\frac{5}{6}}} \right] - 1 \qquad \text{For } 0 \le \sigma_1^2 < \infty \qquad (3.35)$$

And for a spherical wave:-

$$\sigma_I^2 = \exp\left[ \frac{0.17\sigma_1^2}{\left(1 + 0.167\sigma_1^{\frac{12}{5}}\right)^{\frac{7}{6}}} + \frac{0.225\sigma_1^2}{\left(1 + 0.259\sigma_1^{\frac{12}{5}}\right)^{\frac{5}{6}}} \right] - 1 \quad \text{With } 0 \le \sigma_1^2 < \infty \qquad (3.36)$$

These two expressions are plotted below in Figure 3.31.

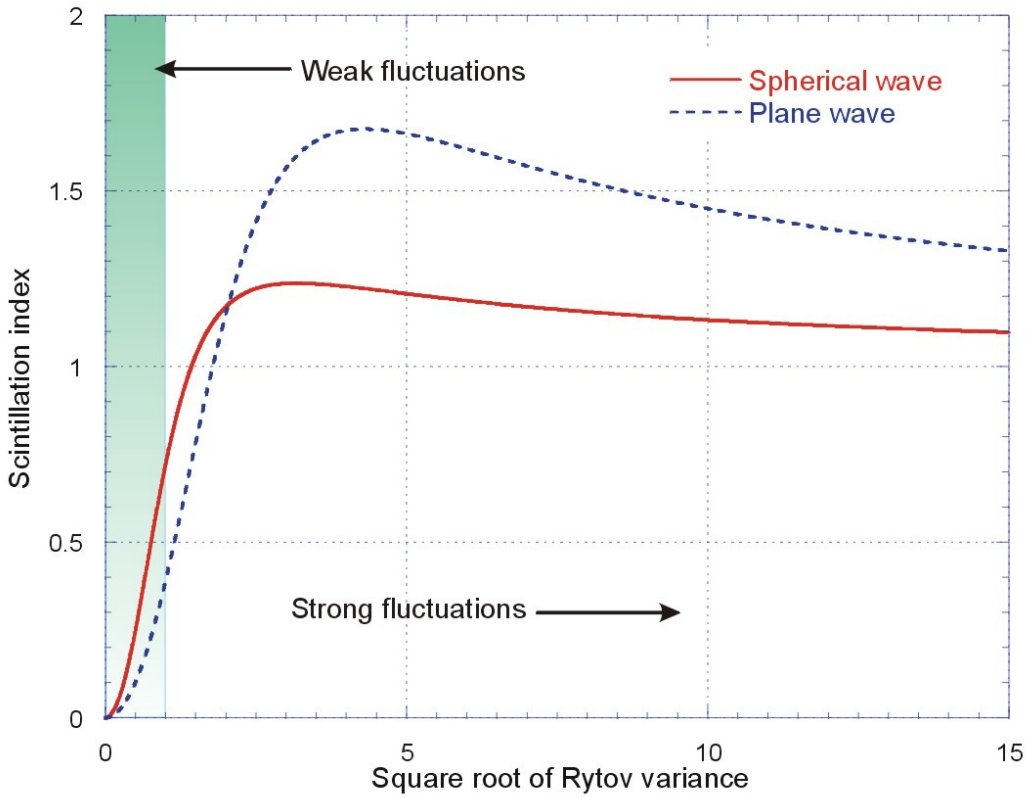


*Figure 3.31. Plot showing the scintillation index plotted against the Rytov variance for a plane and spherical wave. In both cases the scintillation strength increases in proportion to the Rytov variance ($C_n^2$ or L) until a saturation value is reached and then $\sigma_I^2$ decreases, eventually to a value of unity.*

The value of scintillation index increases in proportion with the Rytov variance until it reaches a value somewhat greater than unity in a regime characterised by random focussing, so called because the focussing caused by large scale inhomogeneities achieve their strongest effects. Further increases in turbulence or path length reduce the amount of fluctuations until the scintillation approaches saturation at a value of one.

Saturation occurs due to the effects of multiple scattering causing a decrease in coherence as the beam propagates, eventually resulting in the beam appearing to be made up of multiple extended sources each scintillating with random phases.

In general, the theory of scintillation effects only holds for weak turbulence, i.e., when $\sigma_I^2<0.5$. This limit can easily be reached over transmission paths of 1km when close the ground, however, as $C_n^2$ decreases with altitude, the theory can be used for longer paths at altitude.

### *3.5.6.2 Other important optical effects*

***Image Blur and "Dance"***

It is well known that turbulence induced phase fluctuations in optical wavefronts can give rise to angle of arrival (AoA) fluctuations in the received optical beam. The result of these AoA fluctuations is to cause the incoming wave to be brought to a focus at randomly varying points in the focal plane of the receiver. These points vary over time leading to the familiar phenomenon of image "dance" or "boil".

Additionally the same fluctuations can also give rise to variations in the curvature of the wavefront. This can then cause the incoming wave to be bought to a focus at varying points in front off, and behind the focal plane of the receiver lens.

These situations are shown below in Figure 3.32

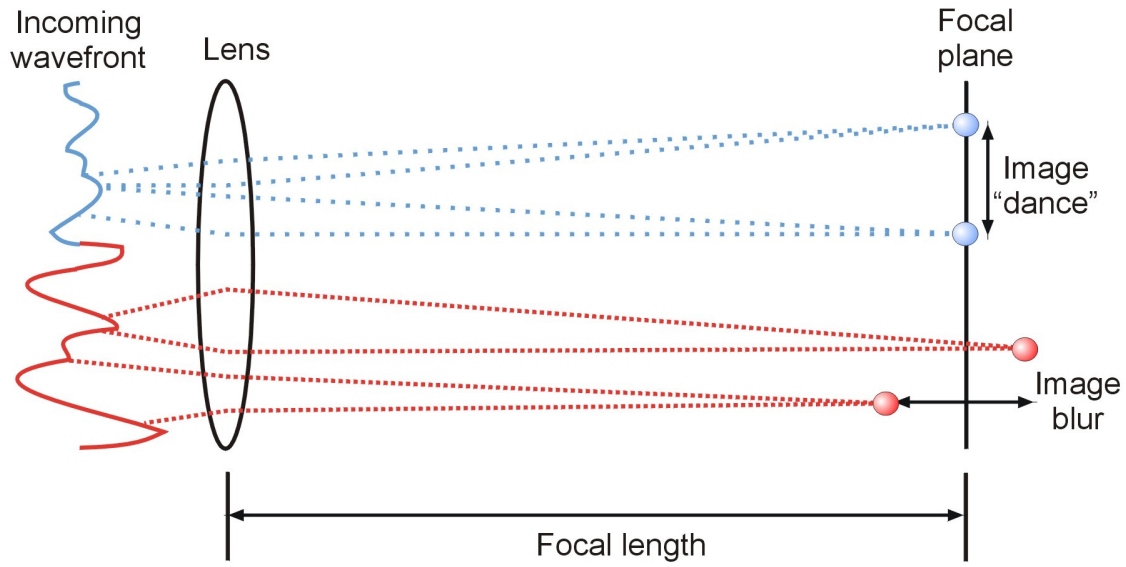


*Figure 3.32. Image blur and "dance". As the angle of arrival changes over time the image moves about in the focal plane appearing to "dance" or "boil". Variations in the wavefront curvature cause an image to be focused randomly about the focal plane.*

The result of these effects is that in a system (such as a QKD system) using point detectors, the angle of arrival can be larger than the optical system can accommodate and the image of the transmitter may appear outside of the detector element and result in a signal loss. In the case of the wavefront radius of curvature the image is defocused, again leading to signal loss in the case of limited detector sizes.

From the point of view of QKD system design there are two important parameters of interest, the strength of the fluctuations and the timescale over which they happen. A knowledge of these parameters allows the construction of adaptive optics systems which can mitigate some of the effects.

For example, angle of arrival fluctuations occur with a frequency spectrum characteristic of the transverse wind velocity along the transmission path. A knowledge of the frequency spectrum can help in the design of adaptive optics systems, specifically feedback loop bandwidth and actuator response times.

#### *3.5.6.3 Dispersion and pulse spreading*

Atmospheric effects can also present problems with pulse spreading. This phenomenon can be due to atmospheric dispersion which will tend to smear out the pulse depending on several factors such as the spectral and polarisation content of the pulse. In addition the turbulent effects can cause the beam to traverse different paths through the atmosphere to the receiver. The combined effect of this can be to increase timing jitter and decrease bandwidth of the channel. It should be noted that these effects are usually very small and a QKD system is generally limited by other factors such as detector response times.

#### *3.5.6.4 Implications for QKD system design*

The effect of scintillation at the receiver of an optical communications system is that whilst the receiver aperture receives the same average power as in the case of no scintillation, the destructive interference can reduce the power below the receiver threshold whilst the constructive interference areas can saturate the receiver. In addition, the distorted phase fronts can lead to decreased efficiency when coupling into single, or low order, mode receivers. A further effect to consider with pulsed systems is that for short pulse systems, the scintillation frequency can also interfere with pulse detection.

The overall effect of scintillation is signal fade and short term signal loss and again as in the case for beam wander, the fading and loss cause absolute signal loss in a QKD system due to the reduced fluence in the beam.

#### *3.5.6.5 Mitigation of scintillation effects*

Scintillation is a problem that is not easy or even possible to solve without a lot of work and investment, however, large improvements in signal to noise ratio can be made with modest investment in engineering and design. A few specific methods are listed below:-

***Multiple beams and receivers (space division multiplexing)***

Several systems have been proposed for free-space communications using multiple input-output (MIMO) methods. This appears to act as a kind of aperture averaging effect. Whilst MIMO appears to be a common technique in free-space optical communications a MIMO QKD system has yet to be built. Although at least one has been proposed [65].

***Aperture averaging***

This is a simple method whereby the receiver aperture is increased beyond the irradiance coherence length. For example, if the receive aperture is a point detector, the output signal will follow the random nature of the scintillations, but if the aperture is increased, the scintillations will tend to average over the aperture and the scintillation will be reduced. Furthermore, a larger aperture can collect more signal (and more noise) [66].

***Adaptive optics***

Adaptive optics such as deformable mirrors are commonly used in astronomical telescopes and recently in FSO systems. QKD implementations have also been proposed and reported. Although there are limitations to the use of these systems, they provide a definite advantage.

## 3.6 Random number generation

Random number generation plays a vital role in a wide variety of applications; including numerical simulation, gaming and cryptography. In the field of cryptography, keys are formed using a stream of random numbers and failure to supply numbers that are sufficiently random can seriously compromise the security of the cryptographic system. Furthermore, the most secure cryptographic techniques require random numbers to be supplied at a very high bit rate. For example, in the case of a One Time Pad (OTP) encryption scheme, the number of random bits required is equal to the number of bits of information to be encrypted.

A perfect random number generator should be unpredictable; this means that even with knowledge of all the bits generated up to some point in time, it is not possible to guess the value of the next bit with better than 50% success rate. Correlation coefficients provide a measure of the deviation of a real bit generator from this ideal; for example a 1% correlation coefficient implies that knowledge of one bit allows another one to be predicted with 50.5% success rate.

Random numbers are the basis for the keys which are shared by BB84 protocol based QKD systems. In general, BB84 QKD requires two sources of random number. The first source resides at Alice and is used to select the output state of the system. In the case of free-space systems this tends to be a choice of polarisations states. The second source of randomness is required at Bob to make the random basis selection for the detection channel. This is often left to chance by the use of a 50/50 non-polarising beamsplitter.

Many different types of random number generator (RNG) have been developed over the years to meet the quality (i.e. randomness) and bit rate requirements of the above applications. In particular, quantum phenomena have often been used to provide inherently random numbers. Devices based on the radioactive decay of elements [67] and the randomness associated with the path travelled by single photons of light passing through a beam splitter [68] [69] have been developed. Although such devices offer truly random number generation, the associated complexity makes high bit rate, low cost, devices impractical.

Random number generators based on a variety of electrical techniques have also been constructed. However, such devices are typically used in applications where low levels of randomness are acceptable. Two typical examples of electrical RNGs are described in [70] and [71].

It is often the case that a random number generator produces a bit stream that appears to be random but nonetheless contains deviations from truly random behaviour. These deviations can take the form of, for example, a bias in the output towards a particular value or a statistical correlation between sampling channels or between temporally separated bit strings. Artefacts such as these can seriously compromise the usefulness of an RNG.

Happily, there exist methods by which these artefacts can be removed. In the case of a bias, one method consists (originally proposed by John Von Neumann) of taking successive output bits and performing an exclusive-OR on them. This will reduce the bias but at the cost of loss of output bandwidth (25% being the best efficiency available with this kind of bias removal).

For statistical correlations a data compression technique can be applied whereby a lossless data compression algorithm is applied to the random bit stream. This technique must increase the entropy of the data in order for the compression to take place or else there would be no compression (of course it is impossible to compress completely random data since there is no redundancy in the data string). Care should be taken with the compression approach since some compression algorithms can produce a predictable output. In addition a carelessly applied algorithm will have artefacts such as file headers which may provide information as to the content or structure of the file.

## 3.7 Single photon detection

### *3.7.1 Introduction*

The ability to detect single photons is desirable in a number of applications where low optical signal levels are encountered, for example, rangefinders, optical communications systems and quantum key distribution systems. There are a variety of devices capable of detecting energies at the single photon level and these include Photo-multiplier tubes, Superconducting transition edge sensors, Superconducting nanowire sensors Avalanche photodiodes and Parametric upconversion detectors. For an excellent review on the subject of single photon detection see [72]. In this thesis the detector of interest is the avalanche photodiode due to its simplicity and widespread use in quantum information systems.

### *3.7.2 Avalanche photodiodes*

The avalanche diode is a device which exploits the phenomenon of avalanche breakdown in semiconductors. Briefly, this process occurs when an electron within the semiconductor gains sufficient energy (due to a high electric field across the device) to produce further (secondary) electrons via the process of impact ionisation.

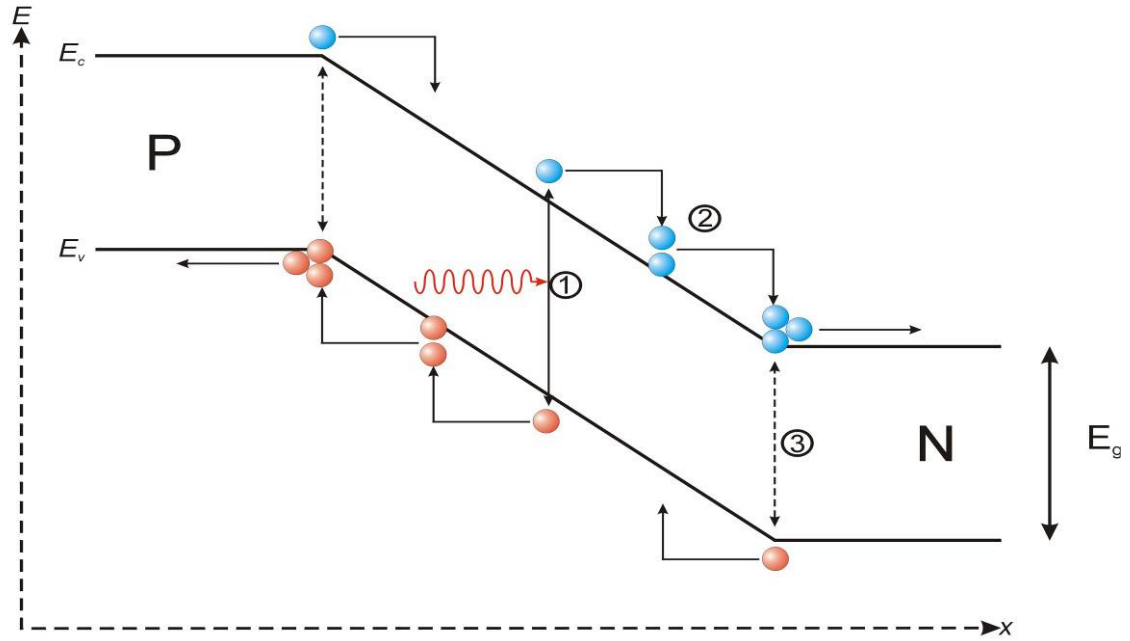


*Figure 3.33. Avalanche breakdown in a semiconductor. 1. An incoming photon generates an electron-hole pair available for conduction. 2. The electron-hole pair are accelerated under the influence of a high electric field and provided they gain energy greater than Eg produce further electrons and holes via impact ionisation. 3. The electrons and holes generated may themselves produce further carriers which also are accelerated and may cause further ionisation events (figure after [73]).*

The secondary electrons may then also gain enough energy to cause a further ionisation. Under the right conditions the resulting cascade produces enough electrons to cause a macroscopic current pulse at the output of the device. A device designed to have the avalanche initiate by photogenerated electron-hole pair is known as an avalanche photodiode device. When these devices are biased above avalanche breakdown, they can be used for the detection of single incident photons. Such devices are called single photon avalanche diodes or SPADs. The process of avalanche breakdown is explained in Figure 3.33 above and in the following section.

### *3.7.3 Single photon avalanche detectors (SPADs)*

SPADs are avalanche photodiodes which have been optimised for use as single photon detectors. The devices are operated in the so-called Geiger mode which means that they are reverse-biased beyond their avalanche breakdown voltage. The avalanche breakdown point is caused by the feedback of electron and hole impact ionisation intiating a self-sustaining avalanche, i.e. a current that will not stop unless there is an external stimulus (e.g. the removal of the bias voltage or an large increase in temperature). When a photon is absorbed, a self-sustaining avalanche is triggered which continues until the device is reset or quenched, usually by the removal of part of the external bias. Modern SPADs are designed to maximise the area available for absorption of the incoming radiation whilst at the same time possessing a narrow multiplication region which allows a greater control over the high electric field required for impact ionisation to occur. A diagram of a typical SPAD device is shown below in Figure 3.34 together with a profile of the resulting electric field.

The incoming photon impinges on the detector and is absorbed in the intrinsic region (i). A photo-electron is generated which then drifts toward the high electric field region. The photoelectron enters the region and is accelerated across it, possibly gaining sufficient energy between collisions to cause impact ionisation. SPAD devices are usually engineered to produce avalanches from one carrier type only since if both electrons and holes are permitted to avalanche, a feedback process such as that described in stage 3 of Figure 3.33 can cause noise, instability and deterioration of the device response time.

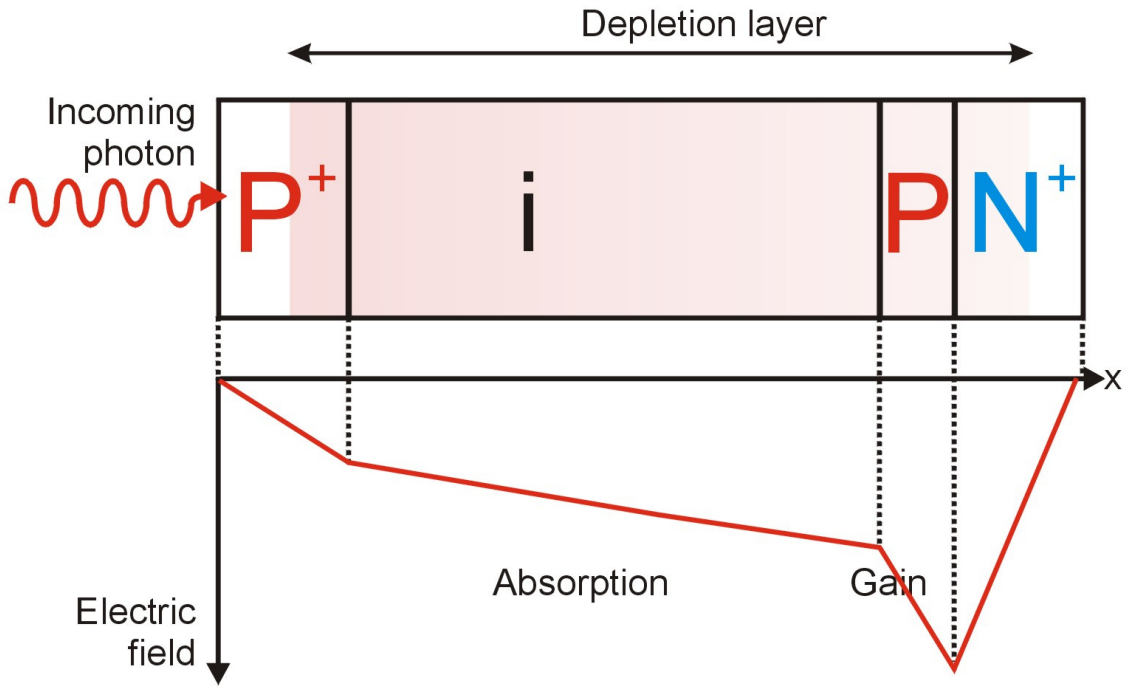


*Figure 3.34. Diagram of a "reach through" SPAD device showing the layered structure. The electric field strength throughout the structure is also shown. (Diagram after [73]). The device is called a "reach through" device since with the application of sufficient reverse bias the depletion region reaches through the intrinsic material to the P+ area and maximises the absorption volume.*

#### *3.7.3.1 SPAD properties*

SPAD devices possess several properties of interest from the QKD design point of view.

***Avalanche voltage***

The avalanche process in SPAD devices will occur at reverse bias voltages greater than the avalanche breakdown voltage, which is highly temperature dependent. For operation in Geiger mode the voltage is typically set a few volts above the avalanche breakdown voltage such that a single incident photon (or dark count) can trigger a self-sustaining avalanche. Conversely, if the device is reverse biased below the avalanche breakdown voltage then the device will quench (i.e. stop avalanching). A typical avalanche breakdown current response from an InGaAs device operating at -65$^{o}$C is shown below in Figure 3.35

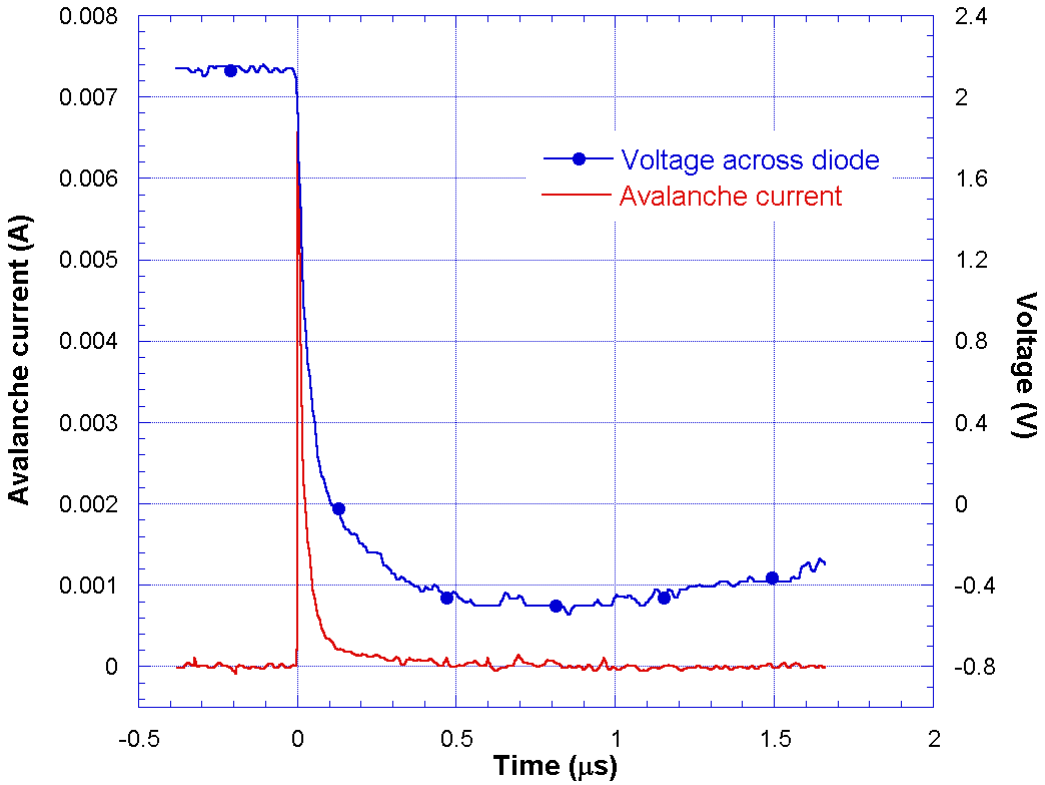


*Figure 3.35. Plot showing a current pulse appearing across a 50Ω sensing resistor during an avalanche in a Princeton Lightwave PGA-400 InGaAs SPAD operating at -65°C with a quenching resistor of 330kΩ. The marked trace shows the voltage across the device during the same time period.*

***Detector efficiency***

This figure allows estimation of the single photon detection efficiency and is generally regarded as the product of two factors, the quantum efficiency, or the probability that an incident photon will generate an electron-hole pair and the avalanche probability which indicates the probability of a given electron-hole pair generating an avalanche.

***Dark current***

Every detector will possess a leakage current caused by thermally generated carrier within the detector material. This is known as a "dark current" and it can cause random avalanching of the device. A detector typically has a figure of merit called dark count probability which characterises this source of noise. The thermally generated electrons can be reduced by cooling the SPAD device, however, this can lead to increased afterpulsing effects, particularly in InGaAs devices.

***Response time and bandwidth***

The avalanche device, like any other diode will posses a finite bandwidth due to various characteristics such as carrier transit times, parasitic capacitance effects and avalanche build up times.

In addition, once the avalanche has taken place, the device must be quenched and the bias voltage must recharge to its pre-avalanche level. This all takes time. Another factor which must be considered is the effect of afterpulsing, which although negligible in silicon-based devices, can have a large effect in the longer wavelength InGaAs devices. Afterpulsing is an effect whereby during an avalanche, some carriers are trapped in material defects and released at a later time. If the reverse bias is still applied or has recharged then these released carriers can cause secondary avalanches subsequent to the photo-induced event. Consequently the device cannot be retriggered until the afterpulsing likelihood has dropped to an acceptable level. All of these effects tend to be lumped together into a detector "dead time" during which the detector cannot be retriggered.

### *3.7.4 Quenching and gating*

Once an avalanche has been initiated by an incident photon or a dark count, the process must be terminated before the device can be used to detect the next photon. This is achieved by a process known as quenching which can be implemented in several ways.

***Passive quenching***

Passive quenching can be implemented with a simple circuit such as that shown below in Figure 3.36 **a** .

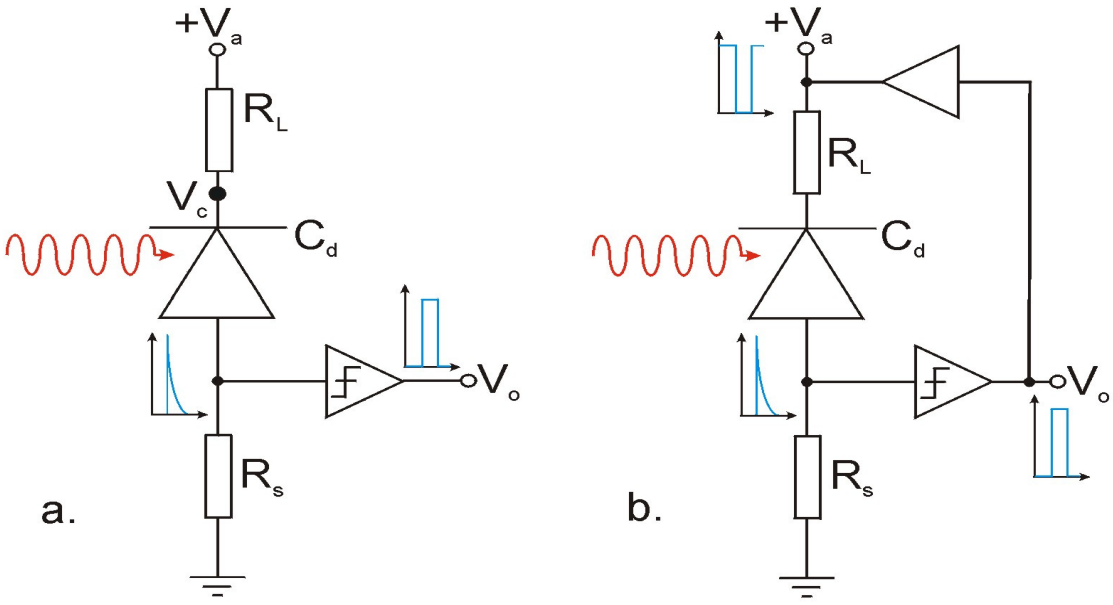


*Figure 3.36. a and b. Simplified passive (left) and active (right) quenching circuits for Geiger mode avalanche photodiodes.*

The SPAD device is reversed bias through a large value resistor, $R_L$. As the avalanche is initiated by the incoming photon, the SPAD begins to conduct and current flows through $R_L$, SPAD and $R_s$, the sensing resistor, to ground.

The current discharges $V_c$ which momentarily dips below the voltage necessary to sustain the avalanche and quenching occurs. The device voltage ($V_c$) then recharges through $R_L$ to $V_a$ ready for the next photon event. Due to the capacitance of the SPAD device and the high value of load resistor (>50kΩ), recharging takes a finite time approximately given by $\tau = R_l C_d$. Here, $C_d$ represents the junction capacitance of the device together with any parasitic capacitance in the circuit.

The output signal appears across the sensing resistor $R_s$ as a small voltage spike which is detected by a comparator which switches on for the duration of the spike and produces a pulse at its output. The comparator is often connected in Schmidt trigger mode such that it acts as a level discriminator as well as an amplifier. A plot of typical SPAD output in passively quenched mode is shown below with the avalanche current spikes clearly tracking the voltage across the device.

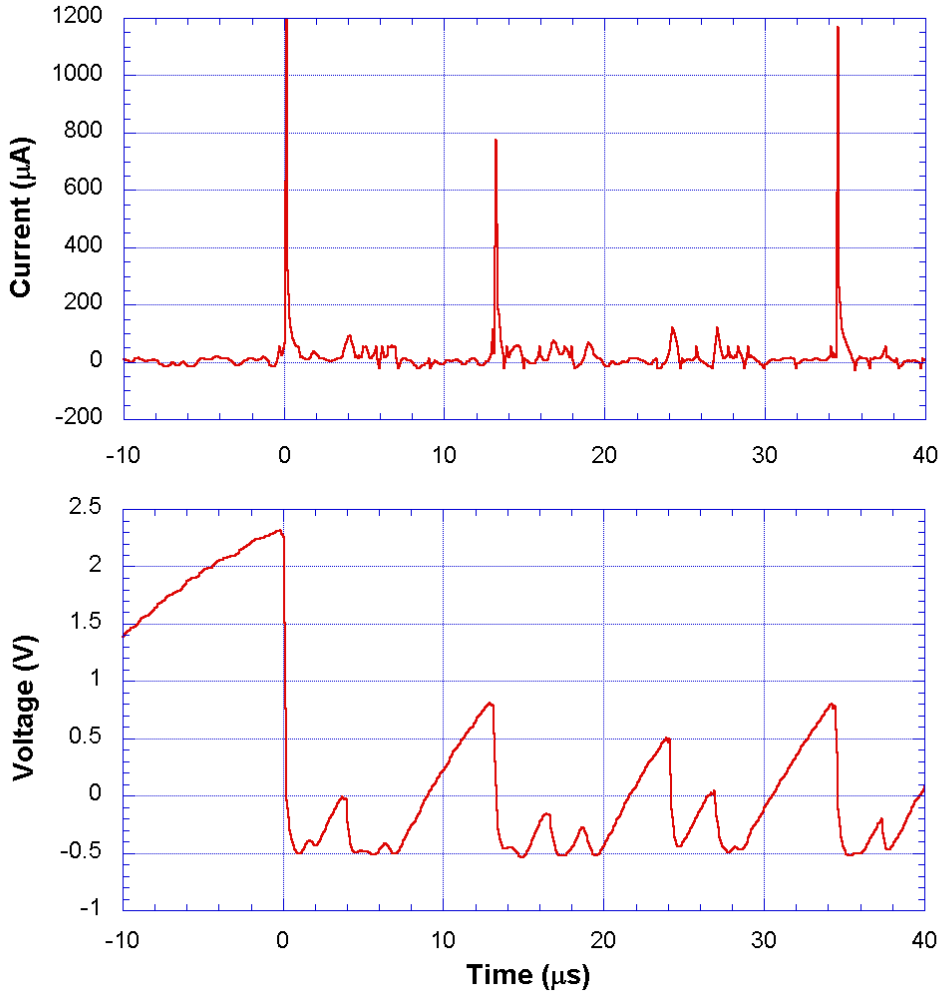


*Figure 3.37. Plot of current through and voltage across a passively quenched ($R_l$=330kΩ) free-running SPAD device (Princeton Lightwave PGA400). Notice how the avalanche pulses track the device voltage.*

### *3.7.4.1 Active quenching*

Active quenching can be achieved with the use of a circuit such as that in Figure 3.36**b**. The avalanche process is similar to that with the passive quenching circuit but the output of the discriminator is used to feed a circuit such as an inverting amplifier whose output is then used to lower the bias voltage, $V_a$. This quenches the avalanche quickly and allows recharging of the circuit through a lower resistance path. Active quenching tends to be much faster than passive and therefore yields a higher detection bandwidth.

### *3.7.4.2 Gating*

Gating is a useful method for controlling SPADs in such a way that the device is armed for a short time before detection and then disarmed a short time later whether or not a detection has been made. The technique is most useful when an incoming signal is expected, for instance in a QKD system. Gating provides several advantages for SPAD operation such as simplicity, noise reduction and mitigation of effects such as after-pulsing. In fact, for practical purposes, some SPADs will only operate efficiently in gated mode.

To implement gating it is necessary only to bias the device just below the avalanche voltage and then apply a short rectangular pulse of sufficient amplitude to take the device bias into the Geiger mode avalanche region. An example of a gated pulse may be seen below in Figure 3.38.

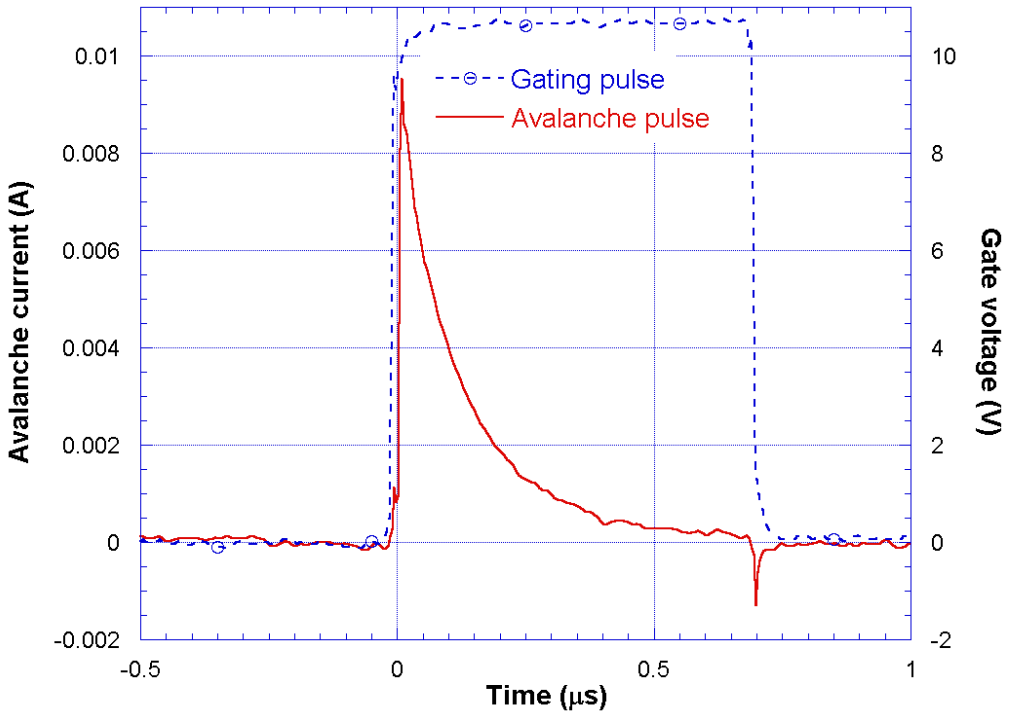


*Figure 3.38. Capture of a SPAD output pulse with its associated gating pulse. Note the capacitive coupling spikes at the beginning and end of the SPAD pulse.*

One problem with gating is the method of applying the gating pulse to the SPAD since the Cathode of the SPAD is at some relatively high voltage (i.e. >100V for Si SPADS and >50V for InGaAs). A popular method is to apply the gate pulse via a small capacitor, however, this can cause large capacitive spikes to form at the start and end of the gate pulse which can be mistaken for legitimate SPAD pulses by a discriminator. There are known methods for removing these spikes such as reducing the *dV/dt* of the gating pulse or using differential detection methods. An excellent review of SPAD quenching circuitry and related issues is given in [74].

### *3.7.5 Time correlated single photon counting.*

Time correlated single photon counting (TCSPC) is a well known powerful statistical sampling technique capable of making measurements at exceptionally low optical power (picoWatt regime) with very fast signals [75], [76].

The method works as follows:

A short laser pulse is emitted in response to a trigger, for instance, from a good quality pulse generator. The trigger pulse is also used to start an extremely accurate clock.

The pulse travels to some distant target and a portion of the pulse is reflected (or in the case of a fluorescence measurement, absorbed and re-emitted) to a detector co-located with the laser. On detection of the reflected pulse the clock is stopped and the elapsed time is logged with high precision by suitable processing electronics.

The process is repeated for a suitable time period until a large number of detections have been made ($\sim\times 10^6$).

At the end of the measurement the laser is disabled and the processing electronics create a histogram of detections with their associated timings. Provided the system has been set up properly such that only one photon per emitted pulse is likely to be detected then the histogram is a faithful reconstruction of the phenomenon under investigation such as the shape of the laser pulse or the lifetime of a fluorescent material.

Since the detection process is an assimilation of collected counts over time (rather than the pulse envelope derived from a conventional analogue detector) the response time of the system is not limited by the detector. In fact the system performance is only limited by the electronic jitter and the dark count of the detector.

The technique is of interest here because the QKD system uses a form of TCSPC to log the arrival times of polarised photons.

In the case of QKD the detector is at a distant location but both emitter and detector communicate by some classical communications channel allowing both terminals to accurately synchronise themselves and create an exact timeline for emissions and detections.

#### *3.7.5.1 Pulse width measurement*

A useful application of TCSPC mentioned above is that of pulse width measurement. This technique is of interest in this thesis since it enables the measurement of fast pulses. The technique is shown in Figure 3.39. An accurate pulse generator is used to initiate an attenuated laser pulse. The laser is coupled via free-space or fibre to a single photon detector. The pulse generator and the SPAD output are connected to the "A" and "B" signal inputs of an HP53310A modulation domain analyser (MDA) respectively.

The MDA is operated in fast histogram mode and as such displays a continuously updated histogram of the time interval between the reception of the "A" pulse and the "B" pulse. This histogram is an accurate reconstruction of the laser pulse and is acquired by the PC via a GPIB interface for later processing.

All pulse width measurements in this thesis are measured in this way unless otherwise stated. Similar measurements could also be made with instruments such as the Sensl HRM-time module, a Picoquant PicoHarp analyser or a Guidetech GT65x series timing card.

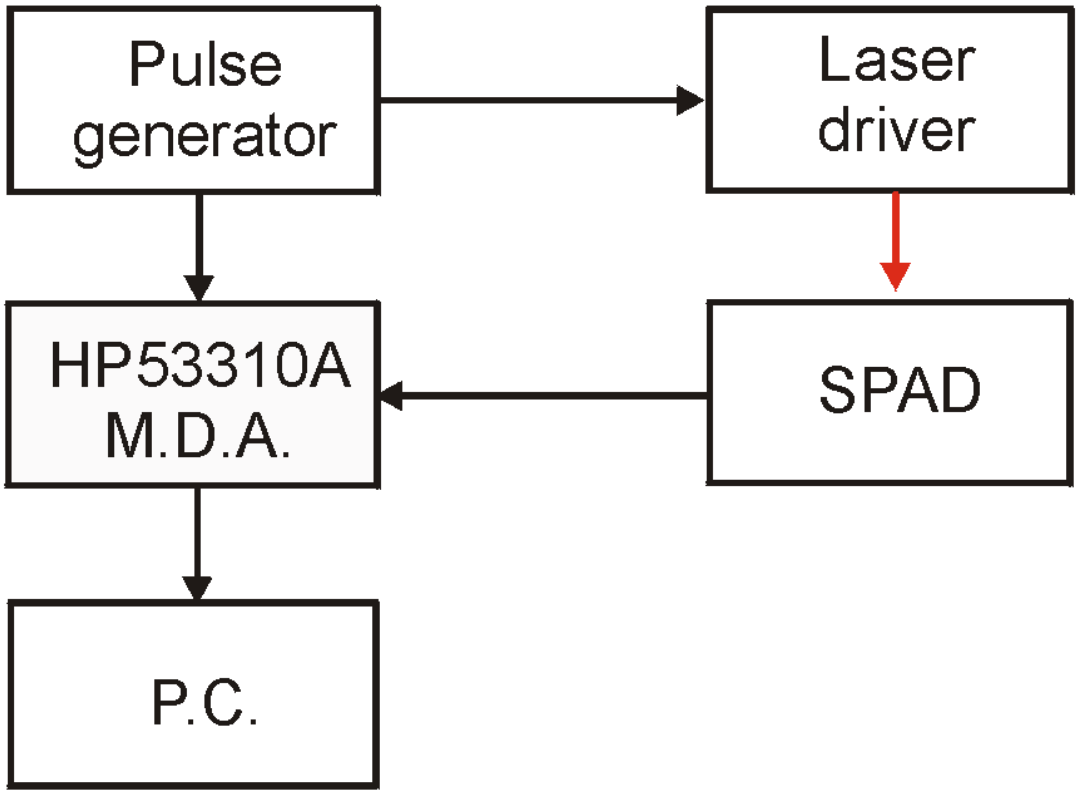


*Figure 3.39. A schematic of a modified TCSPC system for measuring pulse widths.*

## 3.8 Conclusion

Quantum key distribution is a complex process which can theoretically be shown to be unconditionally secure. However, physical realisations of QKD systems require that engineering compromises are made. These can jeopardise system security unless the compromises are made with an awareness of their consequences. In this chapter, the physical basis for QKD has been discussed along with some the principal physical challenges which arise when attempting to build practical systems. Various solutions to these challenges have also been presented. With this knowledge one can build a system and avoid the more obvious pitfalls at the design stage.

### 3.9 Chapter 3 references


[1] R. I. G. Hughes, “The Structure and Interpretation of Quantum Mechanics”, Harvard University Press, First edition 1992. ISBN 0-674-84392-4, (1989).

[2] M. A. Nielsen and I. L. Chuang, “Quantum Computation and Quantum Information”, Cambridge University Press, 2009. ISBN 0-521-63503-9, (2009).

[3] F. Mandl, “Quantum Mechanics”, Butterworths 2nd edition (1957).

[4] Harry Paul, “Introduction to Quantum Optics”, Cambridge University Press, English edition, ISBN 0-521-83563-1, (2004).

[5] W. Heisenberg, “Über den anschaulichen Inhalt der quantentheoretischen Kinematic und Mechanik”, Zeitschrift f¨ur Physik, **43**, p 172–198, (1927).

[6] W. Heisenberg, “The physical content of quantum kinematics and mechanics”, pages 62–84, Princeton University Press, ISBN 0-691-08316-9 (1983).

[7] S Wiesner, “Conjugate coding”, ACM Sigact news, **15**, No.1, 76-88. (1983).

[8] N. Herbert, “FLASH—A superluminal communicator based upon a new kind of measurement”,Found. Phys. 12 1171, (1982).

[9] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned”, Nature (London), **299**, 802 (1982).

[10] A. Peres, “How the no-cloning theorem got its name”, arXiv:quant-ph/0205076v1, (2008).

[11] C. H. Bennett, and G. Brassard, “Quantum cryptography and its application to provably secure key expansion and coin tossing”, IEE International Symposium on Information Theory, St. Jovite, Quebec. (1983).

[12] C. H. Bennett, and G. Brassard, “Quantum cryptography: Public key cryptography and coin tossing”, International conference on computers, systems and signal processing, Bangalore, India, 175 – 179, (December 10-12 1984).

[13] J.G. Rarity, P. R. Tapster and P. M. Gorman, “Free-space key exchange to 1.9 km and beyond”, J. Mod. Opt. **48**, 1887–1901 (2001).

[14] C. Shannon, “Communication in the Presence of Noise”, Proceedings of the IRE, **37**, 1, 10–21, (1949). Reprinted: Proceedings of the IEEE, **86**, No. 2, (1998).

[15] G. Brassard and L. Salvail, “Secret key reconciliation by public discussion”, Advances in Cryptology - Proceedings of Eurocrypt’93, (1993).

[16] L. Tančevski, B. Slutsky, R. Rao and S. Fainman, “Evaluation of the cost of error correction protocol in quantum cryptographic transmissions”, Proc. SPIE, 3228, 322-331 (1997).

[17] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, C. G. Peterson, “Fast, efficient error reconciliation for quantum cryptography”, Physical Review A, **67** (5), pages 052303–1–052303–8 (2003).

[18] P. Grönberg, “Key Reconciliation in Quantum Key Distribution”, Technical report for FOI (Swedish Defence Research Agency), ISSN1650-1942 (2005)

[19] C. H. Bennett, G. Brassard and J-M. Robert, “Privacy amplification by public discussion”, SIAM J. Comput. **17**, 2, (1988).

[20] C. H Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, “Experimental Quantum Cryptography”, J. Cryptology, 5, 1, 3-28 (1992).

[21] D. Gottesman, H-K. Lo, N. Lütkenhaus, J. Preskill, “Security of quantum key distribution with imperfect devices”, Quant.Inf.Comput. 5 325-360 (2004).

[22] Quantum Hacking group at the Norwegian University of Science and Technology, Trondheim. URL:http://www.iet.ntnu.no/groups/optics/qcr/.

[23] Y. Zhao, C. Hang, F. Fung, B. Qi, C. Chen, and H-K. Lo, “Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems”, Phys. Rev. A 78, 042333 (2008).

[24] C. Hang, F. Fung, B. Qi, K. Tamaki, and H-K. Lo, “Phase-remapping attack in practical quantum-key-distribution systems”, Phys. Rev. A 75, 032314 (2007).

[25] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, “The breakdown flash of Silicon Avalanche Photodiodes -backdoor for eavesdropper attacks?” J. Mod. Opt. 48, 2039–2047, (2001).

[26] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, “Trojan-horse attacks on quantum-key-distribution systems”, Phys. Rev. A 73, 022320, (2006).

[27] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Thermal blinding of gated detectors in quantum cryptography”, arXiv:1009.2663v1, (2010).

[28] V. Makarov, “Controlling passively quenched single photon detectors by bright light”, New Journal of Physics 11 065003, (2009).

[29] M. Oxborrow, & A. Sinclair, “Single-photon sources”, Contemporary Physics, **46**, No. 3, 173-206, (May-June 2005).

[30] B. Lounis and M. Orrit, “Single-photon sources”, Rep. Prog. Phys. **68** 1129–1179, (2005).

[31] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail & J. Smolin, “Experimental Quantum Cryptography”, Eurocrypt '90 May 21-24, Arhus, Denmark. Proceedings 253-265, (1990).

[32] H-K. Lo, “Getting something out of nothing”, Quantum Information and Computation **5**, No. 4&5, 413-418, (2005).

[33] A. Muller, J. Breguet, and N. Gisin, “Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over More than 1 km”, Europhys. Lett. **23**, 383, (1993).

[34] P. D. Townsend, J. G. Rarity and P. R. Tapster, “Single Photon Interference in 10km Long Optical Fibre Interferometer”, Electron. Lett., **29** 634-635, (1993)

[35] J.D. Franson and B.C. Jacobs, “Operational system for quantum cryptography”, Electronics Letters **31**, 232-234, (1995).

[36] H-K. Lo and H. F. Chau, “Quantum Cryptography in Noisy Channels”, arXiv:quant-ph/9511025v1, (1995).

[37] D. Mayers, “Quantum key distribution and string oblivious transfer in noisy channels”, Advances in Cryptography—Proceedings of Crypto’96 (Springer-Verlag, New York, 1996), pp. 343-357, (1996).

[38] P. W. Shor and J. Preskill, “Simple proof of security of the BB84 quantum key distribution protocol”, Phys. Rev. Lett. **85**, 441–444, (2000).

[39] N. Lütkenhaus, “Security against individual attacks for realistic quantum key distribution”, Phys. Rev. A **61**, 052304, (2000).

[40] H. Inamori, N. Lütkenhaus and D. Mayers, “Unconditional security of practical quantum key distribution”, arXiv:quant-ph/0107017, (2001).

[41] N. Lütkenhaus and M. Jahma, “Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack” New J. Phys. **4**, 44, (2002).

[42] D. S. Pearson and C. Elliot, “On the optimal mean photon number for quantum cryptography”, Eprint quant-ph/0403065, (2004), http://arxiv.org/ftp/quant-ph/papers/0403/0403065.pdf

[43] W. Y. Hwang, “Quantum key distribution with high loss: Toward global secure communication”, Phys. Rev. Lett. **91** 057901, (2003).

[44] H. K. Lo, X. Ma. and K. Chen., “Decoy state quantum key distribution”, Phys. Rev. Lett. **94** 230504, (2005).

[45] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, Decoy State “Quantum Key Distribution”, Phys. Rev. Lett. **94**, 230504, (2005).

[46] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin, “Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations”, Phys. Rev. Lett. **92**, 057901, (2004).

[47] Chi-Hang Fred Fung, Kiyoshi Tamaki, and Hoi-Kwong Lo, “Performance of two quantum-key-distribution protocols”, Phys. Rev. A **73**, 012337, (2006).

[48] The United States Patent Office defines free space in a number of ways. For radio and radar applications the definition is "space where the movement of energy in any direction is substantially unimpeded, such as the atmosphere, the ocean, or the earth" (Glossary in US Patent Class 342, Class Notes).

[49] Another US Patent Office interpretation is Subclass 310: Communication over free space, where the definition is "a medium which is not a wire or a waveguide".

[50] J. Franson, and B. Jacobs, “Quantum cryptography in free-space”, Optics Letters **21**, 1854–1856, (1996).

[51] Richard J. Hughes, William T. Buttler, Paul G. Kwiat, Steve K. Lamoreaux, George L. Morgan, Jane E. Nordholt, and Charles G. Peterson, “Quantum Cryptography For Secure Satellite Communications”, IEEE Aerospace 2000 Conference, Big Sky, Montana, (2000).

[52] J. G. Rarity, P. R. Tapster, P. M. Gorman and P. Knight, “Ground to satellite secure key exchange using quantum cryptography”, New Journal of Physics **4** 82.1–82.21, (2002).

[53] Michel Riguidel, “Quantum Crypt-Enhancement of AGT Communications Security using Quantum Cryptography”, Report prepared for the European Organisation for the Safety of Air Navigation (EUROCONTROL), Report no. ENST/EEC/QC.12.01.WP3.A, (June 2004).

[54] Kazunori Suzuki; Eiichi Yamada; Hirokazu Kubota; Masataka Nakazawa Optical soliton communication system using erbium-doped fiber amplifiers, Fiber and Integrated Optics, **13**, Issue 1, 45 – 64, (1994).

[55] Joseph. T. Verdeyen. Laser electronics 2nd ed, Prentice-Hall International ISBN 0-13-523655-X, (1989).

[56] J.C.R. Hunt, “Lewis Fry Richardson and his contributions to mathematics, Meteorology, and models of conflict”, Annu. Rev. Fluid Mech. **30**, xiii–xxxvi, (1998).

[57] R. Beland, The Infrared and Electro-optical Systems Handbook, Vol.2 – Atmospheric Propagation of Radiation, Chapter: “Propagation through Atmospheric Optical Turbulence”, 212–232. SPIE Optical Engineering Press, Bellingham, (1993).

[58] N. Kolmogorov. “The local structure of turbulence in an incompressible viscous fluid for very large Reynolds numbers”, R. (Doki) Acad. Sci. U.S.S.R. **30**, 301–305, (1941).

[59] L. C. Andrews, R. L. Phillips, C. Y. Hopen, and M. A. Al-Habash, “Theory of Optical Scintillation”, J. Opt. Soc. Am. A, **16**, 6, (June 1999).

[60] L. C. Andrews and R. L. Phillips, Laser beam propagation through random media, SPIE press, ISBN 0-8194-2787-X, (1998).

[61] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger and H. Weinfurter, Experimental “Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km”, Physical Review Letters, **98**, 010504, (2007).

[62] J. I. Davis, “Consideration of Atmospheric Turbulence in Laser Systems Design”, Applied Optics. **5**, 1, (1966).

[63] A. D. Wheelon, Electromagnetic Scintillation II: Weak Scattering, Cambridge University Press 0521801990, (1990).

[64] R. L. Fante, “Electromagnetic Beam Propagation in Turbulent Media”, Proceedings of the IEEE, vol. 63, 12, (1975).

[65] M. Gabay and S. Arnon, “Quantum Key Distribution by a Free-Space MIMO System”, Journal Of Lightwave Technology, **24**, 8, (2006).

[66] M-A. Khalighi, N. Schwartz, N. Aitamer, and S. Bourennane, “Fading Reduction by Aperture Averaging and Spatial Diversity in Optical Wireless Systems”, J. Opt. Commun. Netw.**1**, 6, (November 2009).

[67] M. Ishida and H. Ikeda, “Random number generator”, Ann. Inst. Statist. Math. Tokyo. **8**, 119-126, (1956).

[68] A. Stefanov; N. Gisin; O. Guinnard; L. Guinnard; H. Zbinden, “Optical quantum random number generator”, Journal of Modern Optics, **47** Issue 4, 595 – 598, (2000).

[69] J. G. Rarity, P. C. M. Owens and P. R. Tapster, “Quantum random-number generation and key sharing”, Journal of Modern Optics, **41**, No 12, 2435-2444, (1994).

[70] Victor S. Reinhardt; Clinton Lew, “High Speed Word Generator”, United States patent no.US5224165, (1990).

[71] Andrew J. Vincze, “Analog-to-digital Conversion Method of Random Number Generation”, United States patent no. US6369727, (1999).

[72] Robert H. Hadfield, “Single-photon detectors for optical quantum information applications”, Nature Photonics **3,** 696-705, (2009).

[73] B. E. A. Saleh and m. C. Teich., Fundamentals of Photonics, Wiley Interscience, ISBN 0-471-83965-5, (Chapter17.4, p666), (1991).

[74] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, “Avalanche photodiodes and quenching circuits for single-photon detection”, Applied Optics **35**, 12, (1996).

[75] Michael Wahl, Time-Correlated Photon Counting, Tech Note TCSPC 1.2, PicoQuant GmbH, (2000).

[76] Becker and Hickl application note, “Time-Correlated Single Photon Counting”, TCSPC1.DOC, (July 2002).

# Chapter 4 - A description of a practical free-space QKD system

## 4.1 Introduction

In this chapter the idea of a typical or "generic" free-space QKD (FSQKD) system is introduced and the functions and sub-systems that go together to make such a system are examined. The idea of a generic system is useful for understanding how FSQKD systems work and also allows comparison with some of the more novel techniques that have been implemented.

In general, a QKD system consists of transmit and receive terminals, termed Alice and Bob respectively (the names betray a historical connection to the nomenclature used in information theory). In this chapter, each terminal and its associated controlling computer are discussed in turn.

In addition, there are ancillary systems required for successful operation which are important enough to warrant separate consideration. Ancillary systems include methods of timekeeping, generation of random numbers and relay optics.

This chapter will review all of these components, along with some practical considerations to be borne in mind when operating in real world scenarios. An example of a typical free-space QKD system is shown below in Figure 4.1.

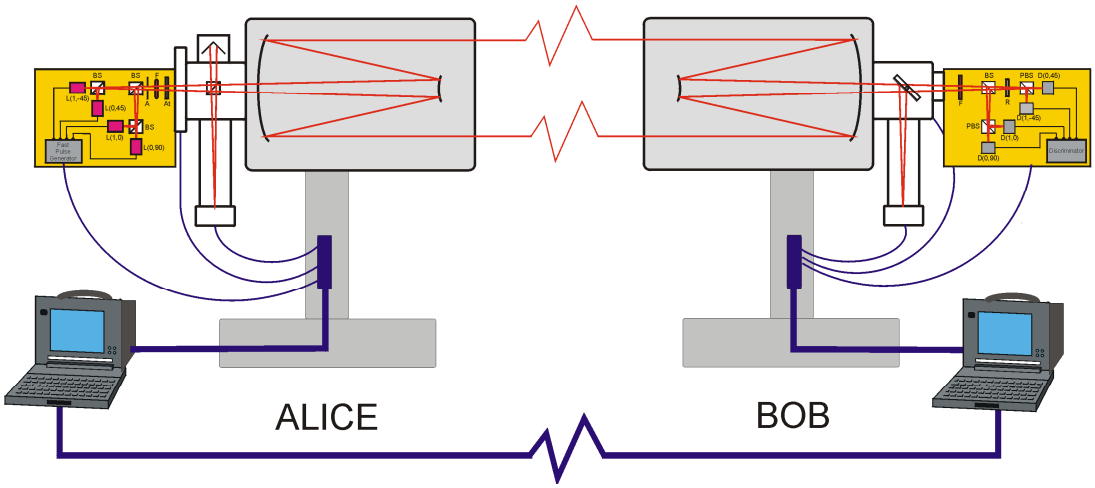


*Figure 4.1. The main components of a free-space QKD system. Alice and Bob are coupled to two telescopes and also interfaced to a controller, usually a computer running the protocol software. The terminals are connected by two channels, a quantum channel carrying the "data" and a classical channel for key reconciliation.*

## 4.2 The transmitter

The term Alice is used to describe the complete QKD transmitter subsystem which consists of:

- Computer controller and interface
- Optical sources and drive electronics
- Optical system

A diagram of the complete Alice transmitter subsystem showing the major components is shown below in Figure 4.2

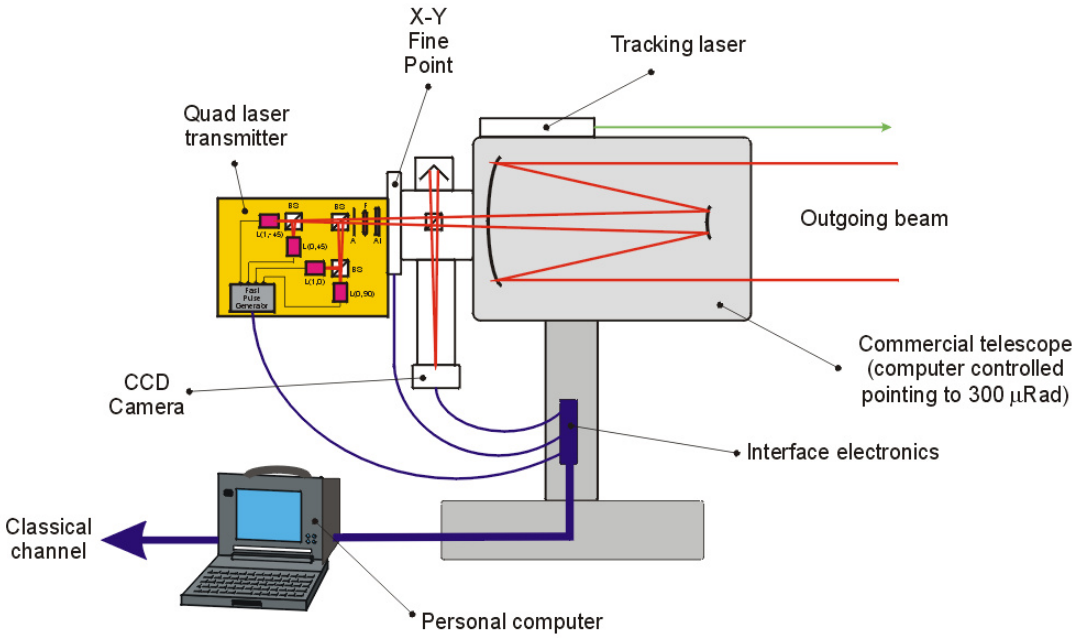


*Figure 4.2. An example of a complete free-space QKD transmitter system, or Alice for short.*

### *4.2.1 General overview of transmitter operation*

The QKD transmitter described here is designed to implement the four-state, weak coherent pulse, polarisation encoded version of the BB84 protocol. However, with some simple modifications it could also be made to operate with B92, Decoy state and SARG protocols. Since these modifications involve changes to the protocol or electronics, the optical layout is much the same for any of the above protocols. Key exchange operations proceed as follows:-

***Computer controller and interface***

The Alice transmitter is invariably controlled by a computer of some description running a proprietary operating system such as Windows (although several research groups are known to prefer a Linux-based solution).

Personal Computers are commonly used, but some systems have been developed to the point where processing and control are implemented using FPGA or ASIC chips (for example see [1] & [2]). The computer is also used as a data processor for much of the key reconciliation process.

Whilst individual implementations of the protocols differ, the controller will typically initiate an output signal in response to a random input and a predetermined set of rules governed by the key exchange protocol in use. A general example of QKD system structure is shown below.

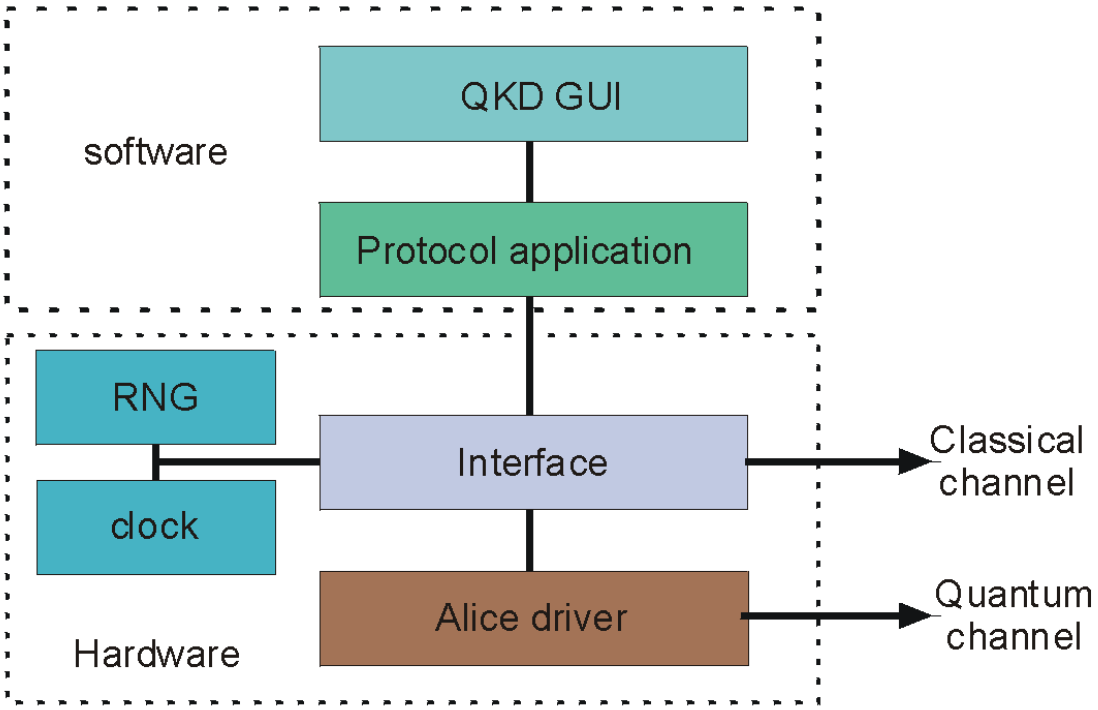


*Figure 4.3. A conceptual diagram of a QKD system showing how the software and hardware are interfaced. A graphical user interface (GUI) controls the QKD protocol application which outputs instructions via some interface within the controlling computer. These instructions are interpreted by the Alice driver and result in the outputs to the Quantum channel. The computer interface also manages classical communication channel for key reconciliation. The random number generator is the "information" source whilst the clock provides synchronisation.*

***Optical sources and drive electronics***

In the generic system, a set of four optical sources are used; with two sources allocated to each of the output polarisation bases (e.g. source 1&2 – diagonal basis, source 3&4 – rectilinear basis). The sources are chosen such that they possess similar properties. For instance, they must be matched in terms of spatial and spectral distribution of radiation and must possess the required signal bandwidth.

Several source devices have been tested for use in QKD such as light emitting diodes (LEDs), vertical cavity surface emitting lasers (VCSELs) and resonant cavity LEDs (RCLEDs), but edge emitting semiconductor laser diodes tend to be favoured, particularly as they possess a high intrinsic linear polarisation ratio.

Having been output from the computer in a standard form (for example, TTL or ECL bit stream), the data is required to be converted to a suitable form for initiating optical pulses. To this end the data pulses are subjected to amplification, pulse shaping and delay stages before being applied to the optical sources.

***Optical system***

The Alice optical system is designed to take the light emission from the multiple optical sources and couple them together into one homogenous beam suitable for launching into free-space. An example of a generic transmitter for the four-state BB84 protocol is shown below in Figure 4.4.

Light pulses from sources 1&2 are coupled together spatially by a polarising beamsplitters (PBS). Some leakage occurs through the unused beamsplitter port but is of no concern, provided it is dumped efficiently and does not leak out of the transmitter enclosure. A similar optical layout is provided for sources 3&4.

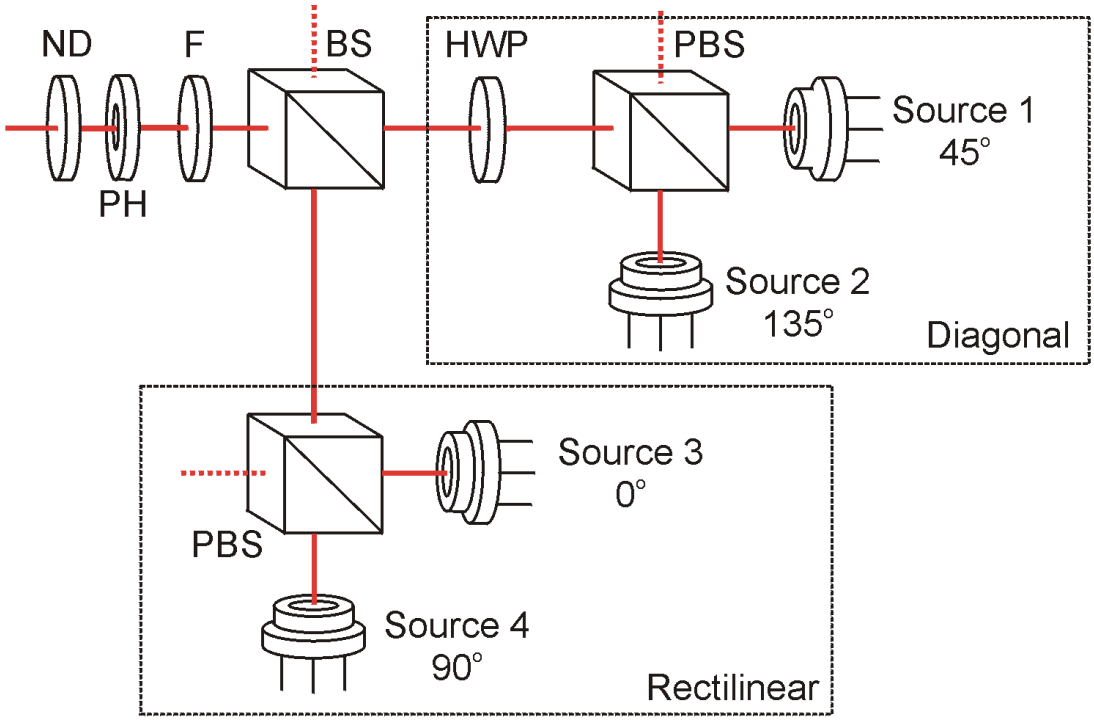


*Figure 4.4. Diagram showing the optical system of a "generic" QKD transmitter. Four sources are coupled together to form a single attenuated beam at the output.*

The two resulting beams are then coupled together in the same way as before, except that the diagonal basis is rotated by 45$^{o}$ using a half wave plate (HWP) before the coupling beamsplitter (BS). Neglecting the half wave plate would require the entire diagonal basis arm of the transmitter to be physically rotated. Alternatively, the individual sources would have to be rotated before coupling together. This would lead to the emission from the diagonal basis transiting two beamsplitters containing 45$^{o}$ surfaces instead of one and result in polarisation errors for the diagonal basis. Having been coupled together spatially, the optical beam now continues through a narrowband optical filter (F) and on to a pinhole (PH). The pinhole has the effect of spatially filtering the beam such that all four components appear to have come from a single source. The resulting beam is then passed through an attenuator (ND) to reduce the fluence of the beam to the correct average photon number (μ) for a QKD system (see chapter 3 for a discussion of μ value). Finally the beam is coupled to free-space via some form of telescope (dealt with later in this chapter).

### 4.3 The receiver

The term Bob refers to the complete QKD receiver sub-system, which consists of:

- Optical system and detectors
- Signal processing electronics
- Computing and processing
- Housekeeping (APD biasing and temperature control).

A diagram of the complete Bob receiver showing the major components is shown below in Figure 4.5.

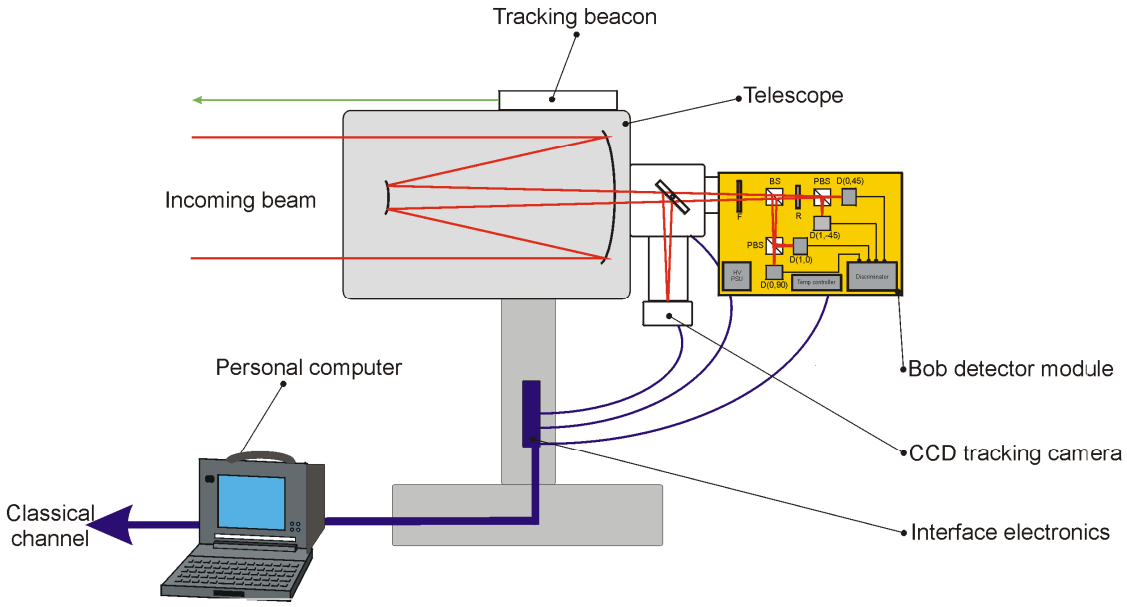


*Figure 4.5. A complete free-space QKD receiver system, or Bob for short.*

### *4.3.1 General overview of receiver operation*

The BB84 protocol is a four state protocol with the individual signal states encoded into two sets of two orthogonal polarisations. A suitable receiver will therefore require the ability to detect this type of signal encoding. All BB84 receivers will tend to be a version of a generic receiver, that is, whatever their construction or hardware they must fulfil identical functions. An example of a generic receiver is shown below in Figure 4.6.

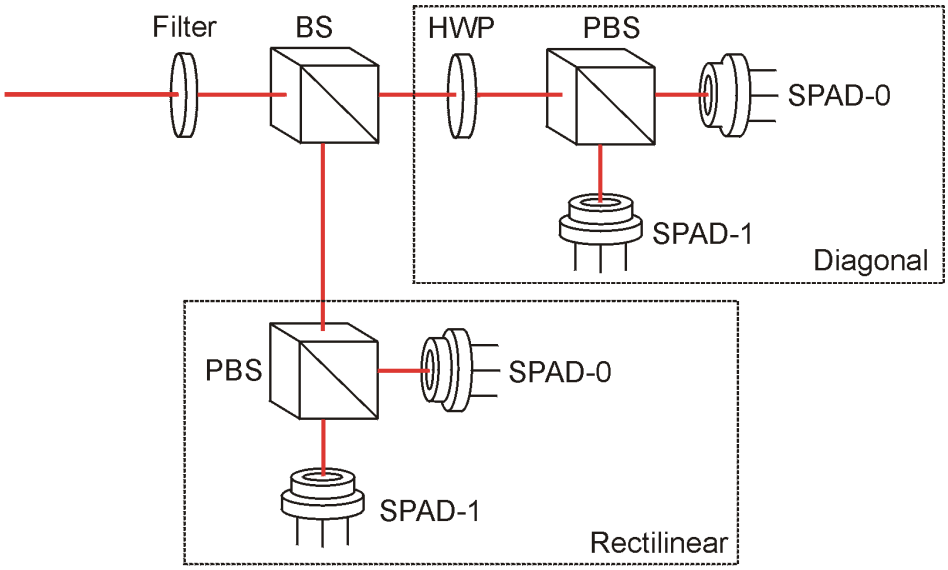


*Figure 4.6. A "generic" QKD receiver optics. Incoming light is filtered and passed through a passive optical system for analysis and measurement in one of four single photon detectors.*

Measurement and detection takes place as follows:-

Incoming light, having been gathered and focussed or collimated by a telescope (not shown) is spectrally and spatially filtered to remove background and passed to the first analyser (BS). On arrival at this beamsplitter the photon makes a "decision" on which detector arm to enter.

Provided the beamsplitter is of good quality and coated properly the result is that incoming photons are equally and randomly split between the two detector arms. Put simply, the first beamsplitter acts as a random choice generator between analysers [3].

The photon then continues into one or other of the detector arms and, ignoring the half wave plate for the time being, will encounter a second beamsplitter. However, this time the "choice" of detector arm is made on the basis of polarisation state.

Vertically polarised photons will enter the "1" detector whilst horizontally polarised photons will enter the "0" detector, thus allowing the receiver to discriminate between horizontal and vertical polarisation states.

The final act of the incoming photon is to be absorbed at the surface of the SPAD detector and create a “click” in the detector electronics.

For simplicity, the two analysers are usually made identical and to further reduce complexity, instead of rotating the analyser arm by $45^{o}$, a half wave plate is inserted such that any incoming photons of the diagonal basis are rotated to a rectilinear base. In this way, one of the analysers is made sensitive to the diagonal basis and the receiver system becomes capable of analysing the four required states for BB84. The use of a passive beamsplitter is an improvement over previous systems which tended to use polarisation modulators which were bulky, lossy and required high-voltage power supplies. A passive random choice also enables larger throughput to the detectors. However, like other receivers, 50% of the incoming photons are lost since they will enter the incorrect analyser.

It should be noted that one could also use left and right circularly polarised light for a basis set and merely substitute the half wave for a quarter wave plate.

***Computing and processing***

The absorption of the photon results in a small pulse at the output terminal of the detector. This pulse is then amplified and passed to a discriminator circuit (both circuits are often combined in the form of an ultra-fast comparator circuit) which usually form part of the detector electronics. The discriminator output is then passed to an interface where the incoming pulse is recorded with respect to its time of arrival, polarisation state and detection basis. The controlling computer then initiates communication with Alice on an open channel and exchanges information (not bit values) on the time and basis of each detection. This allows the two parties to extract an identical list of bit values.

***Housekeeping***

The Bob module generally contains the necessary electronics for additional “housekeeping” tasks. For example, the receiver uses avalanche photodiodes which require biasing, often at high voltages. In addition, to minimise thermal noise in the detector the devices are cooled aggressively (typically to $<-20^{o}C$ for Silicon SPADs or $<-50^{o}C$ for InGaAs SPADs [4]). Therefore the detectors are mounted on thermoelectric coolers usually connected to some form of temperature controller. Fan-cooled heat sinks provide the final cooling stage.

## 4.4 Ancillary systems

***Telescopes***

The telescope is the front end of the transmitter and receiver systems and should reflect the application to which the system is put. For instance, for short range applications (<4km), a simple Newtonian telescope with, say, a 50mm aperture may be sufficient.

However, as transmission distances increase and the atmospheric effects become more dominant the aperture of the telescope may need to be increased, subject to the limitations discussed in chapter 3 concerning beam wander, diffraction etc. For an example of differing telescope systems one can compare [5] & [6]. In the former experiment, a comparatively short range free-space experiment, both input and output telescopes consisted of 100mm diameter aperture telescopes. One-way active tracking was implemented in this experiment by using a reference beam incident on a quad detector. Error signals were amplified and fed to a controller via a Personal Computer which controlled a steerable output mirror. The beam size was also adjusted such that beam diameter was large enough to cover the receiver aperture despite turbulence induced beam wander.

In the latter, a very long range experiment, the transmitter telescope consisted of a single achromatic lens of aperture of 150mm used to collimate the output from a single mode fibre. In contrast, the receiver utilised a 1m diameter Ritchey-Chrétien astronomical telescope with a focal length of 39m. Both of the telescopes in the latter experiment used active tracking for optimum coupling of the beam.

Another factor in the choice of telescope is wavelength of operation, for example, if a system is operating in the near infrared part of the spectrum, a commercial amateur grade astronomical telescope may not have suitable optics for transmission of light outside of the visible band. This is not a problem at the transmitter end of the system where the fluence of the beam can be adjusted to compensate for the signal loss (subject to upper limits set by security analyses). However, at the receiver, the beam can be highly attenuated and even small losses can have a large effect on system efficiency. The transmission spectrum of a Meade Schmidt-Cassegrain telescope of the type used in [7] is shown below in Figure 4.7.

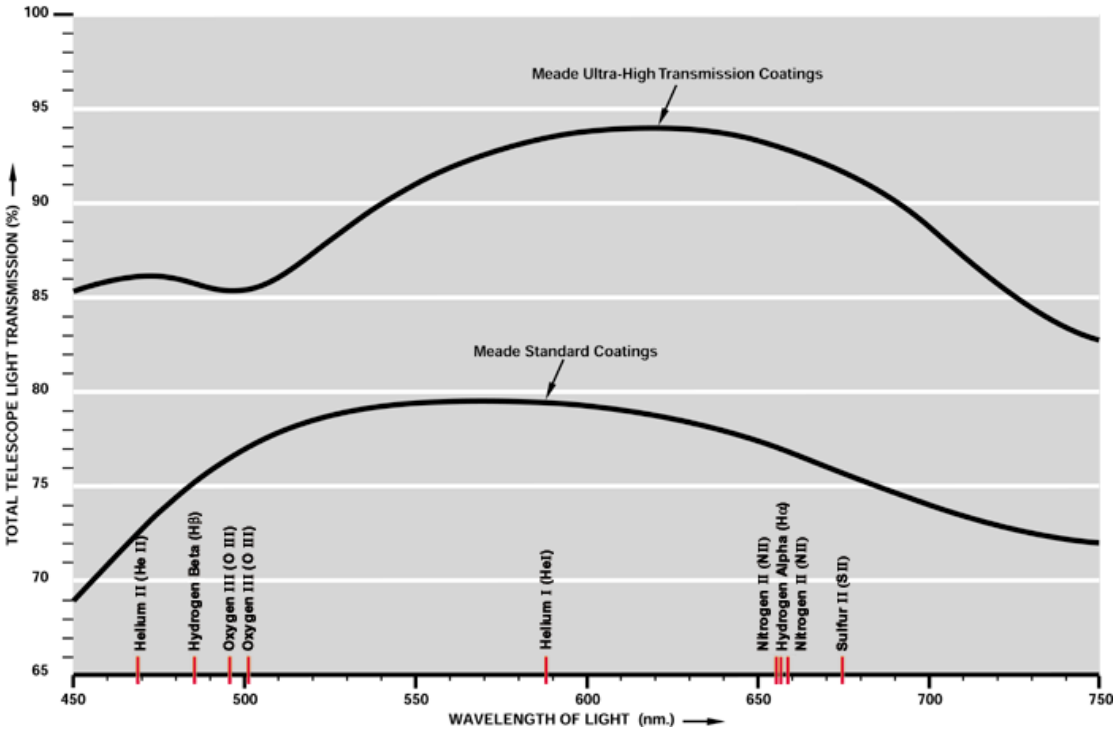


*Figure 4.7. Transmission spectrum of commercially manufactured Meade telescopes. Note that whilst transmission in the visible spectrum is >70%, this figure falls off at longer wavelengths (Figure-Meade Instrument Corporation).*

***Random number generation***

The random number generator provided with most computer systems is actually a pseudorandom generator (PRNG). A PRNG contains a seed and uses a deterministic algorithm to generate random outputs from the seed. Normally the algorithm is public, so if an attacker knows the seed, all the outputs can be predicted. For cryptographic applications, the security of a PRNG depends on the assumption that the attacker has limited computational power available. For robust security analysis and in real life this is not always the case. In these situations a “strong” random number generator is required which produces high quality random numbers. This can be done in a variety of ways. A brief discussion of random number generation is given in section 3.6, whilst development of a random number generator suitable for use in a QKD system is described in section 6.3.

***Timekeeping and synchronisation***

QKD can be regarded as a form of time-correlated photon counting system in that photons are transmitted from Alice at a certain time and detected at Bob a short time later. The emission and detection times are measured extremely accurately and stored so that later on in the key exchange process the times of departure from Alice and the times of arrival at Bob can be correlated and a raw key generated.

There are several ways in which the required level of synchronisation can be achieved:

- Bright pulse

  In some free space quantum key generation systems (for example [1] & [14]) the single photon data transmission is preceded by the emission of a bright optical pulse. The detection of this pulse serves the purpose of preparing Bob for the potential imminent arrival of a photon within a fixed time window.

- Global positioning system (GPS) clock

  To avoid the extra complexity of bright pulse generation some systems (for example [15]) have been known to use accurate GPS clocks to synchronise local clocks at each terminal.

- Phase locked loop (PLL)

  Another synchronisation method used ([5] & [7]) is to initiate a phased lock loop such that Alice and Bob are both synchronised. Both Alice and Bob terminals contain extremely accurate oven controlled crystal oscillator (OXCOs) which operate at nominally the same frequency.

  Bob and Alice are then synchronised using a software implemented phase-locked loop. Synchronisation has two layers (1) A software implemented PLL which is used to ensure that the Alice and Bob systems both have clocks that are operating at the same frequency and (2) a removal of $2\pi$ phase ambiguities by prefacing data blocks with headers of known data which in the case of [5]&[7] is a pseudo-random bit sequence. Synchronisation to better than 1ns can be achieved by this method.

## 4.5 Conclusion

In this final chapter of section 1 of this thesis the main components of a free-space QKD system have been introduced and discussed, including transmitter, receiver and major subsystems. The description has utilised the idea of a generic system which provides a basis for understanding some of the more complex methods of solving implementation problems.

## 4.6 Chapter 4 references


[1] J. Bienfang, A.J. Gross, A. Mink, B.J. Hershman, A. Nakassis, X. Tang, R. Lu, D.H. Su, C.W. Clark, C.J. Williams, E.W. Hagley, and J. Wen, "Quantum key distribution with 1.25 Gbps clock synchronization", Optics Express **12**, 2011–2016, (2004).

[2] D Stucki, N Gisin, O Guinnard, G Ribordy and H Zbinden, "Quantum key distribution over 67 km with a plug&play system", New Journal of Physics **4** 41.1–41.8, (2002).

[3] J. G. Rarity & P. R. Tapster, "Cryptographic Receiver", U.S. Patent No. 6028935, February 22, (2000).

[4] G. S. Buller and R. J. Collins, "Single–photon generation and detection", Journal of Measurement Science and Technology, **29**, 012002, (2010).

[5] J. G. Rarity, P. R. Tapster, and P. M. Gorman, "Free-space key exchange to 1.9 km and beyond", J. Mod. Opt. **48**, 1887–1901, (2001).

[6] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km". Phys. Rev. Lett. **98**, 010504, (2007).

[7] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P.M. Gorman, P.R. Tapster, and J.G. Rarity, "Quantum cryptography: A step towards global key distribution", Nature **419**, 450, (2002).

[8] M. Ishida and H. Ikeda, "Random number generator", Ann. Inst. Statist. Math. Tokyo. **8,** P119-126, (1956).

[9] A. Stefanov; N. Gisin; O. Guinnard; L. Guinnard; H. Zbinden, "Optical quantum random number generator", Journal of Modern Optics, **47,** 4, 595 – 598 (2000).

[10] J. G. Rarity, P. C. M. Owens and P. R. Tapster, "Quantum random-number generation and key sharing", Journal of Modern Optics, **41**, 12, 2435-2444, (1994).

[11] V. S. Reinhardt; C. Lew, “High Speed Word Generator”, United States patent no.US5224165, (1990).

[12] A. J. Vincze, “Analog-to-digital Conversion Method of Random Number Generation”, United States patent no. US6369727, (1999).

[13] P. R. Tapster and P. M. Gorman, “Apparatus and Method for Generating Random Numbers”, United Kingdom patent filing, Patent no.0603523.2, (2007).

[14] R. J. Hughes, J. E. Nordholt, D. Derkacs and C. G. Peterson, “Practical free-space quantum key distribution over 10 km in daylight and at night”, New J. Phys. **4**, 43, (2002).

[15] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter & A. Zeilinger, “Entanglement-based quantum communication over 144km”, Nature Physics, **3**, 481 – 486, (2007).

# Chapter 5 - Early work – Malvern to Munich, 1998 – 2002.

## 5.1 Introduction

This is the first chapter in section 2 of this thesis and deals with early practical work in the field of QKD. Much of the work described in this and the following chapters took place in the context of working within a team at what is now QinetiQ (Malvern) over the course of a decade from 1998 to 2008.

Footnotes are used to delineate between work which was the sole responsibility of the author and work done as part of a team. There are also a few occasions where work done by colleagues is included because it was an essential part of the system development or intimately related to the author's contribution. These are also highlighted by footnotes.

## 5.2 History

QKD research at QinetiQ can trace its ancestry to some of the initial experiments in the field. Several teams at Malvern were already investigating phenomena of quantum entanglement, single photon interference, squeezed light, photon counting and photon statistics. The breakthrough came in 1992 however, with the publication by John Rarity, Paul Tapster, G Massimo Palma and Artur Ekert of the first laboratory demonstration of entanglement based QKD [1]. After 1993, although entanglement research continued, QKD research suffered a hiatus until the start of the European Union funded EQCSPOT collaborative project in late 1998, which is where the full involvement of the author in QKD research begins.

## 5.3 Breadboard short range free space system[5]

Free-space QKD work commenced at Malvern with the requirement to construct a short range breadboard system as part of Work package Three of the EQCSPOT collaborative project. The design of the system was intended as a demonstration of free-space QKD over several kilometres using the BB84 protocol [2].

[5] During the construction of this system, the author was responsible for all optical hardware, drive electronics and trials organisation.

Additionally the system was designed to be capable of withstanding high transmission losses and yielding final key rates at the level of kilobits per second. This work is summarised in the paper by the Malvern group in [3]. In these early days, little work on free-space QKD had been reported and virtually no off-the-shelf components were available. This situation necessitated some innovative design of both optics and electronics.

### 5.4 The breadboard Alice transmitter

The transmitter was constructed on a $1m^2$ optical breadboard and designed to switch the polarisation of short laser pulses between the four required polarisation states at a rate of 10MHz. The light source was a pulsed laser diode from Picoquant (LDH-8-1-135 Laser Head [4]) capable of producing short (100ps) pulses of 635nm light at repetition rates up to 80MHz. The short pulse length was chosen to be shorter than the timing jitter introduced by the detectors (>500ps). The laser output was split into four beams using non-polarising beamsplitters and then directed through four acousto-optic switches followed by fixed half-wave plates set for the four polarisations of $0^0$, $45^0$, $90^0$, $135^0$. A diagram of the Alice apparatus is shown below in Figure 5.1.

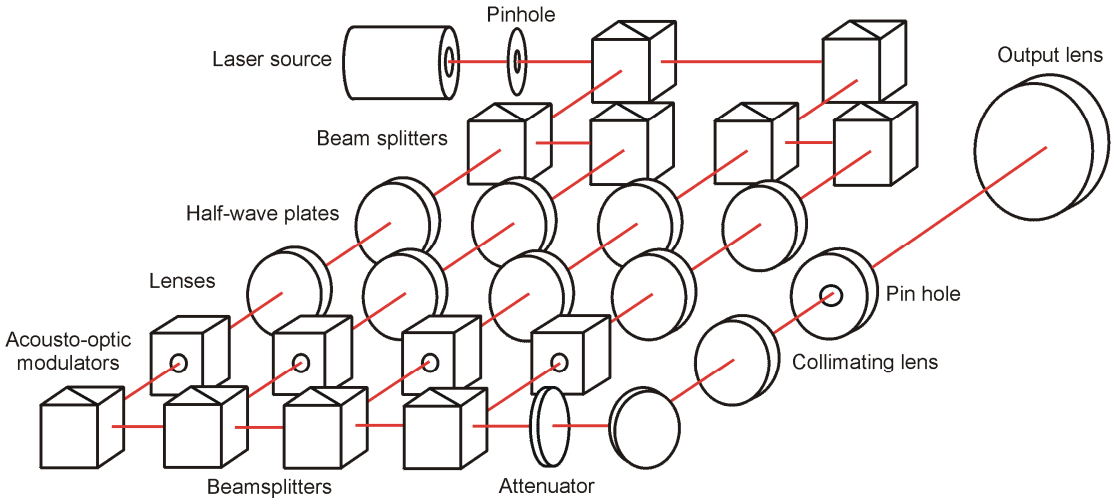


*Figure 5.1. Diagram of the breadboard Alice. A single source is split into four identical beams which are then modulated using acousto-optic modulators.*

Optical switching of the beams was accomplished with the use of four independently addressable acousto-optic switches which were randomly switched using computer-interfaced drivers synchronised to the laser pulses. For this implementation of the system, the random numbers used for the switching were generated from a long (100Mbits) file of pseudo-random numbers stored in the Alice computer.

The four beams (of different polarisations) were then recombined and collimated using output optics consisting of a focussing lens (×5 microscope objective) and 15μm pinhole acting as a spatial filter to ensure all recombined beams were indistinguishable. This was followed by a collimating air-spaced doublet lens of 100mm diameter and focal length 300mm. The resulting output beam diameter was of order 25mm allowing collimation to better than 40μradians.

The pulses were strongly attenuated within the apparatus using neutral density filters until the average photon number ($\mu$) per pulse was less than 0.1. This guaranteed that very few output pulses contained more than one photon. This type of classical approximation of a single-photon source is discussed in chapter 3. A photograph of the physical realisation of the breadboard Alice is shown below in Figure 5.2.

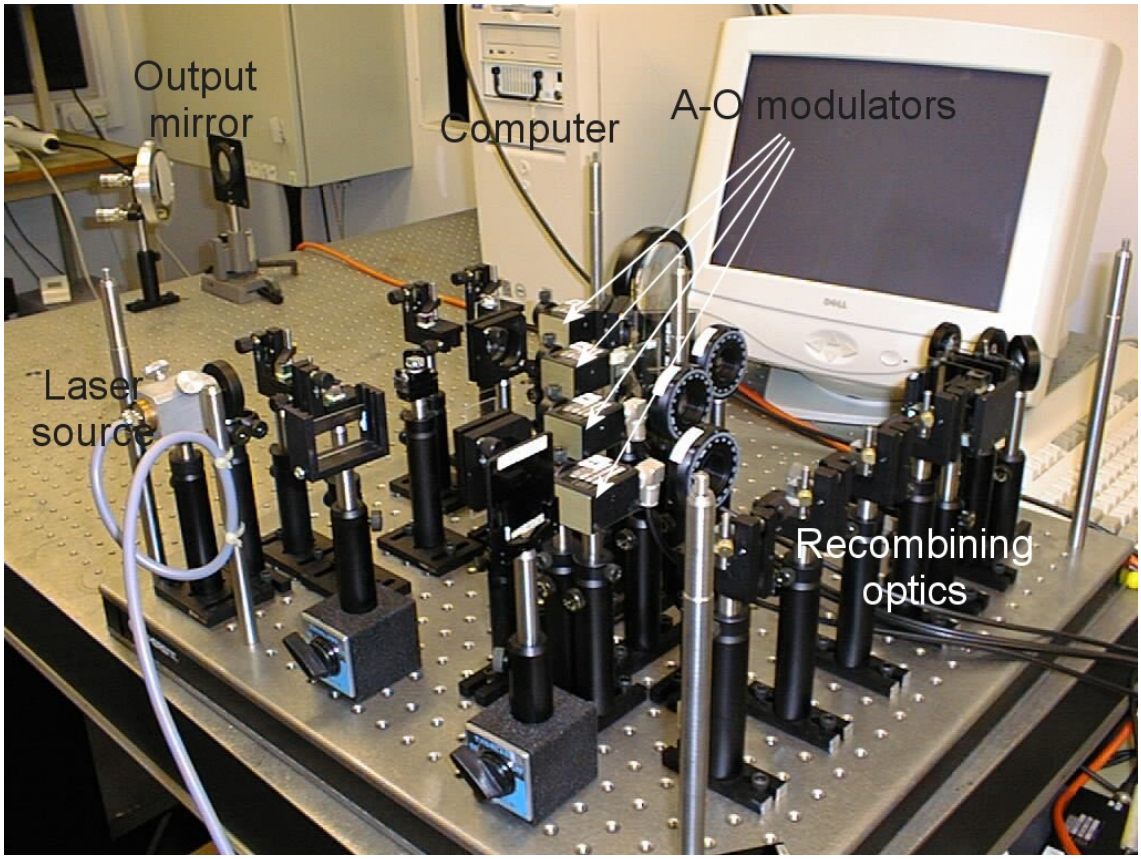


*Figure 5.2. Photograph showing the Alice breadboard in situ at the Pershore laser range. The major components are labelled.*

## 5.5 The breadboard Bob receiver

Like the transmitter, the receiver apparatus was also constructed on a $1m^2$ optical breadboard. In the experimental receiver (Figure 5.3 below) the incoming beam was collected in a 100mm doublet lens and recollimated to a diameter of order 1mm with a long-pass optical filter (F) being used to restrict background visible light. The collimated beam was then split into two by a non-polarising 50/50 beamsplitter (NPBS). This beamsplitter acts as a passive random switch directing the photons through either a half-wave plate (HWP) set to provide $45^0$ of polarisation rotation or a delay path of 3ns. The delay allowed discrimination of the two measurement bases by detection timing (described in [5]). Within the $45^0$ arm a further quarter wave plate (QWP) was used to correct for birefringence effects in the transmitter beamsplitters.

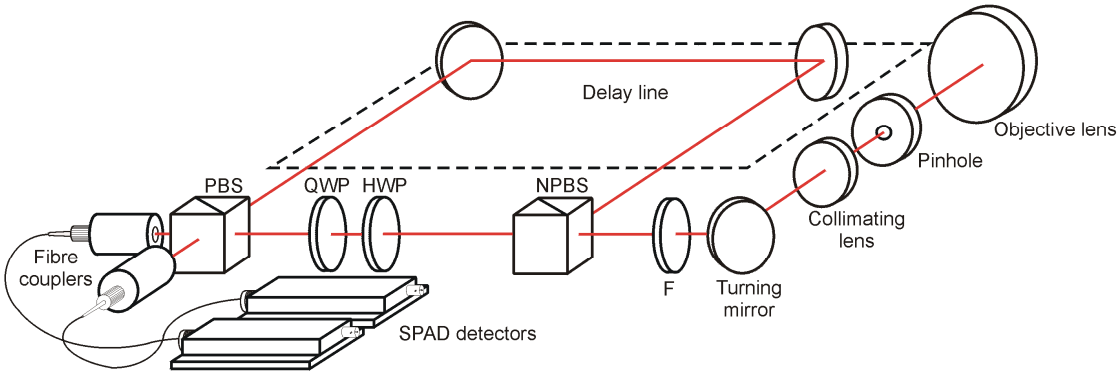


*Figure 5.3. The Bob receiver layout. An optical delay line was used to time multiplex the detectors thus saving on hardware costs. The half-wave plate was used to rotate the polarisation of the incoming light by $45^o$ whilst the quarter wave plate was used to compensate for birefringence errors in the transmitter optics.*

The twin beams were recombined and analysed in a polarising beamsplitter to determine the measured bit values. The light exiting the polarising beamsplitter was collected in two free space-fibre optical couplers and travelled in a pair of multimode fibres to twin Silicon photon-counting modules (EG&G SPCM AQR121 FC) [6]. The overall optical detection efficiency of this receiver was measured as 7±1% (as compared with a quoted detector efficiency of 70% at 650nm). A photograph of the Bob breadboard may be seen below in Figure 5.4.

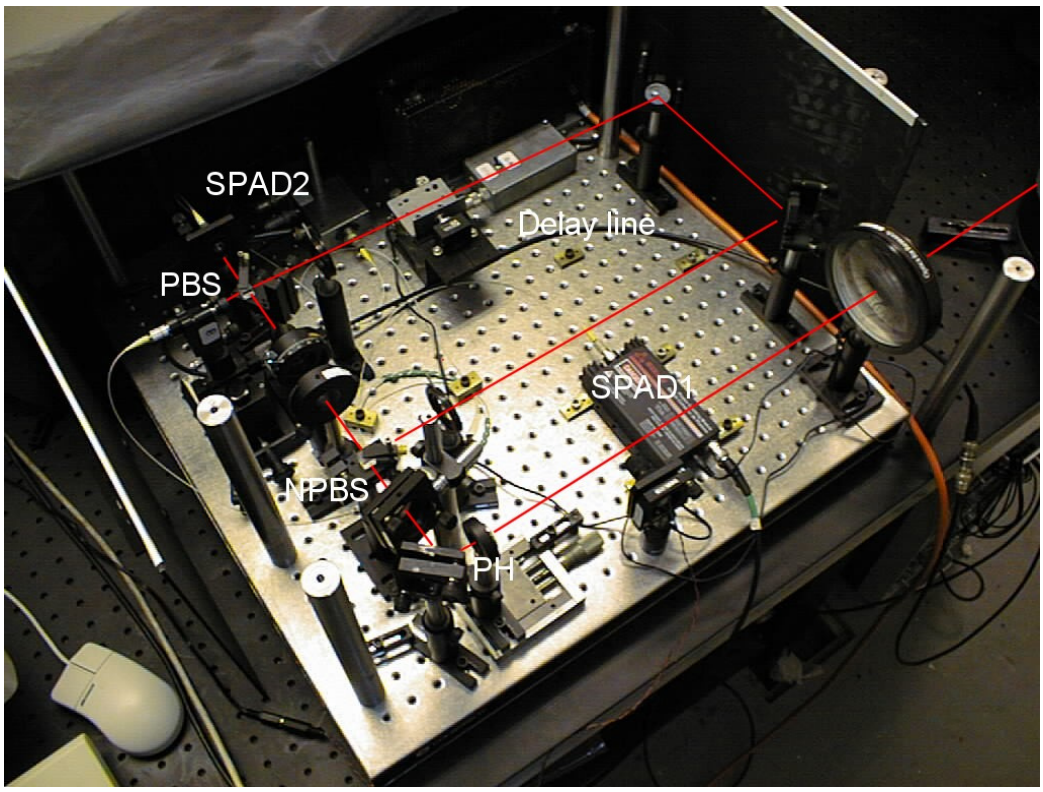


*Figure 5.4. The Bob breadboard mounted to an optical table at the Pershore laser range in November 1999. The incoming optical path is shown in red.*

### *5.5.1 Interface hardware*

Both transmitter and receiver were controlled by Dell Optiplex GX1 computers each containing a single Intel Pentium II microprocessor (350MHz CPU clock rate) and running a standard installation of Windows 98. All timing and control software was implemented in Labview software.

In the Alice computer a Nudaq PCI7300 digital input/output card [7] provided an interface to an electronic driver which produced the signals required to the optical hardware. Meanwhile, at the Bob computer, the time of arrival of each photodetection was recorded using a two channel time digitisation card (Guide Technology GT653).

## 5.6 Software and Protocol Implementation[6]

In parallel with the hardware development, a set of software programmes were developed for implementing QKD. The programmes were designed to implement the BB84 protocol complete with sifting and error correction routines. In addition, some useful diagnostic software was developed. In this section, these aspects of the system are discussed including the novel synchronisation method employed by the system.

[6] Paul Tapster was responsible for software writing on this project. However, design of both software and hardware was necessarily a two way process between engineer and programmer.

### *5.6.1 System synchronisation*

The need for extremely accurate synchronisation arises because Alice and Bob will ultimately compare lists of photons with known polarisations sent at known times.

In other free space quantum key generation systems (e.g. [8], [9]) the single photon data transmission is preceded by the emission of a bright optical pulse. The detection of this pulse serves the purpose of preparing Bob for the potential imminent arrival of a photon within a fixed time window.

The QinetiQ system does not use this approach and thereby does away with the need for an extra optical system that must be aligned and synchronised. The QinetiQ synchronisation system operates on three levels:

Firstly, the internal computer clocks are referenced to a pair of local 10MHz quartz crystal oscillators with a stability of 1 part in $10^8$ (Guide Technology GT300 frequency standards).

Secondly, a software implemented phase locked loop (PLL) is used to ensure that the Alice and Bob systems both have clocks that are operating at the same frequency

Thirdly, a routine for the removal of $2\pi$ phase ambiguities by prefacing data blocks with headers of known data is applied.

The process described here is an ideal one where everything progresses smoothly. The individual stages of the process can be observed for diagnostic purposes using the software tools supplied. The software and diagnostics are described in a separate section.

***Acquiring lock***

Alice sends a set of pulses lasting for 10ms. Bob detects a fraction of these photons and compares their arrival time relative to the nearest clock pulse edge of the local clock, using the GT653 timing card.

An estimated arrival time is made in a software based clock which corrects for time-of-flight delay and intrinsic phase differences between the Alice and Bob clocks. The purpose here is to match the frequency and phase of the Bob system clock with that of the Alice clock.

The average delay in arrival time is determined and used to correct the parameter values used in the software clock. This process is repeated several times until Alice and Bob are synchronised.

Although Bob has four detectors the GT timing card used for accurate timing measurement has only two data (and one clock) input channels.

To get circumvent this difficulty detectors are linked in pairs with the output from one of the detectors is delayed by 4ns relative to the other. A histogram of the resulting timing distribution of detected events is generated by measuring the signal arrival time in the GT card relative to the synchronized clock pulses. The distribution of arrival times in each channel of the GT card has a double-peaked shape where each peak represents counts from one of the detectors, as shown in Figure 5.5.

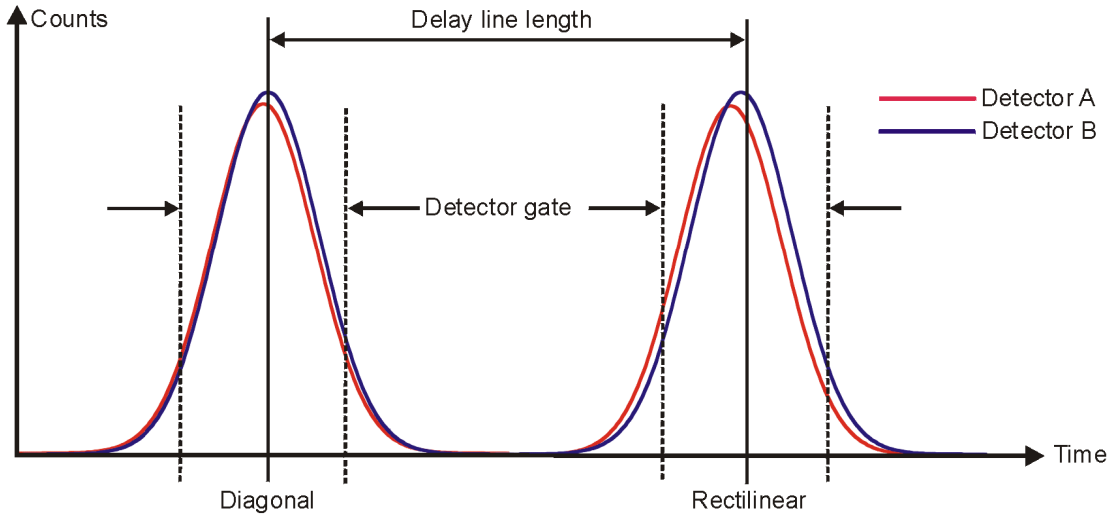


*Figure 5.5. A schematic histogram of the distribution of events from 4 detectors into 2 timing channels where one detector in each pair is delayed. Dotted lines denote the position of timing windows and the situation depicted represents a stable PLL.*

The second set of peaks in the timing distribution represents events detected in the second (delayed) detector of each pair. Therefore the polarisation of a detected photon is inferred according to which peak and in which channel the event is recorded. This timing distribution can be viewed using a diagnostic program called "PLLtest" described later. The PLL is set by using two timing windows, where the separation of the windows matches the known delay introduced between detectors. The phase of the software clock is adjusted until the ratio of counts inside the timing window to those outside exceeds a threshold value (fixed in the software). When this ratio has remained stable for 10 seconds the PLL is considered locked and Alice and Bob synchronised.

***Maintaining Synchronisation***

Once the PLL is set Alice and Bob have synchronised the relative phase of their clocks but there are potential phase ambiguities (the time of flight from Alice to Bob could be many clock cycles and Alice and Bob must be sure they are referencing the same clock pulse). This is particularly a problem due to the way that data is sent. Data transmission is controlled by using 4 bits of a digital input/output card (DIO) where each bit represents one Alice channel.

A buffer of data values is generated and the bit values sent to the Alice unit synchronously with the clock. However, loading and reloading of the data buffer takes time and during this pause (of an inexact period of time) the synchronisation can slip such that Alice and Bob will no longer know exactly which pulse they are referring to. In order to rectify this problem data is organised into blocks, each prefaced by a header containing a pseudo random bit sequence (PRBS) generated from a known algorithm. A recurring pattern of 511 pulses is sent for 40ms. Although there is considerable transmission loss of data, Bob can correlate his detected events with the expected PRBS. The process is repeated with a 1023 bit PRBS to allow unambiguous pulse timing identification. The system is then tested using a 2047 bit PRBS. This process takes around 110ms to complete. The amount of data that can then be sent is then determined by the buffer size used by the DIO card and typically this lasts for 700ms before the buffer is refilled. Another batch of header and data is then started and the process continues until all the data has been sent.

### *5.6.2 Software and diagnostic programs.*

A series of software programs were written to exchange keys and access certain sub-systems in order to perform diagnostics in the set-up and alignment process of the QKD system. The following programs being particularly relevant:

| Program name | Function | Location |
|---|---|---|
| Receivermaster.exe<br>ReceiverSlave.exe | Controls the Bob receiver, ensures synchronisation between Alice and Bob, Collects data and communicates with master computer. | Bob |
| Transmittermaster.exe<br>TransmitterSlave.exe | Takes random number data from master. Controls optical output from Alice unit during synchronization and encodes random number onto optical channels. | Alice |
| Rate Counter.exe | Displays the count rate in channels A and B of the timing card. | Bob |
| PLL test.exe | Allows behaviour of the PLL to be observed and controlled | Bob |
| ExeServer.exe | Allows connection between Alice and Bob slaves . | |

*Table 5.1. A list of programs for use in exchanging keys and diagnosing problems.*

***Receiver.exe, ReceiverSlave.exe***

Runs automatically on system start up and waits for communication from the master computer before attempting to establish the PLL.

Communication with the master computer is performed using the agreed protocol.

When asked by the master communicates its status. ReceiverSlave collects photon events for one block when requested by the master and then subsequently passes a list of detected events to the master computer where key distillation takes place.

***Transmitter.exe, TransmitterSlave.exe***

This program loads automatically upon system start-up but waits for a signal from the transmitter master before commencing. This program controls the optical output from the transmitter head. All the processes for synchronization, header and block data transmission described earlier are carried out – pulse all lasers, then pulse individually in a fashion consistent with the random number file supplied by the transmitter master. TransmitterSlave does not communicate directly with ReceiverSlave and therefore knows nothing about Bob's state, but relies on all control being governed by the master computers.

***RateCounter.Exe***

This program gives both a graphical and numerical representation of the detected count rate in the two channels of the timing card. This is particularly useful when optically aligning the transmitter and receiver where maximising the count rate in channels A and B is the way of obtaining optimum alignment. For channels A and B a horizontal bar progresses across the screen to represent increasing count rate. The scale of this bar adjusts automatically so that changes in the rate are most easily observable.

***PLLtest.exe***

This program displays graphically the behaviour of the phase locked loop. The locking process is as described in section 5.6.1. A screenshot of the program front panel is shown in Figure 5.6. The program has 2 graphical displays showing the double-peaked time histogram for the two channels of the timing card and a phase diagram.

In the histogram the total width of the distribution, the resolution and timing window properties such as width and separation, are displayed and can be controlled using the parameters on the left of the screen. The histogram shown in Figure 5.6 shows timing the timing distribution for channels A and B each with two peaks from the presence of 2 detector outputs with a relative delay. The timing windows used to gate incoming pulses are shown as vertical lines on either side of the centre of each peak.

***Stable condition:***

When first started the display may be featureless as the system adjusts the virtual clock to match that of Alice. As the system homes in on the correct values large peaks in the data may drift across the display, eventually resolving into two peaks that are stabilised about the centre.

As the PLL stabilises the Lock indicator at the bottom of the panel gradually changes in colour from red to green to show a firm timing lock between transmitter and receiver. This program requires a total count rate of less than 60kHz to operate.

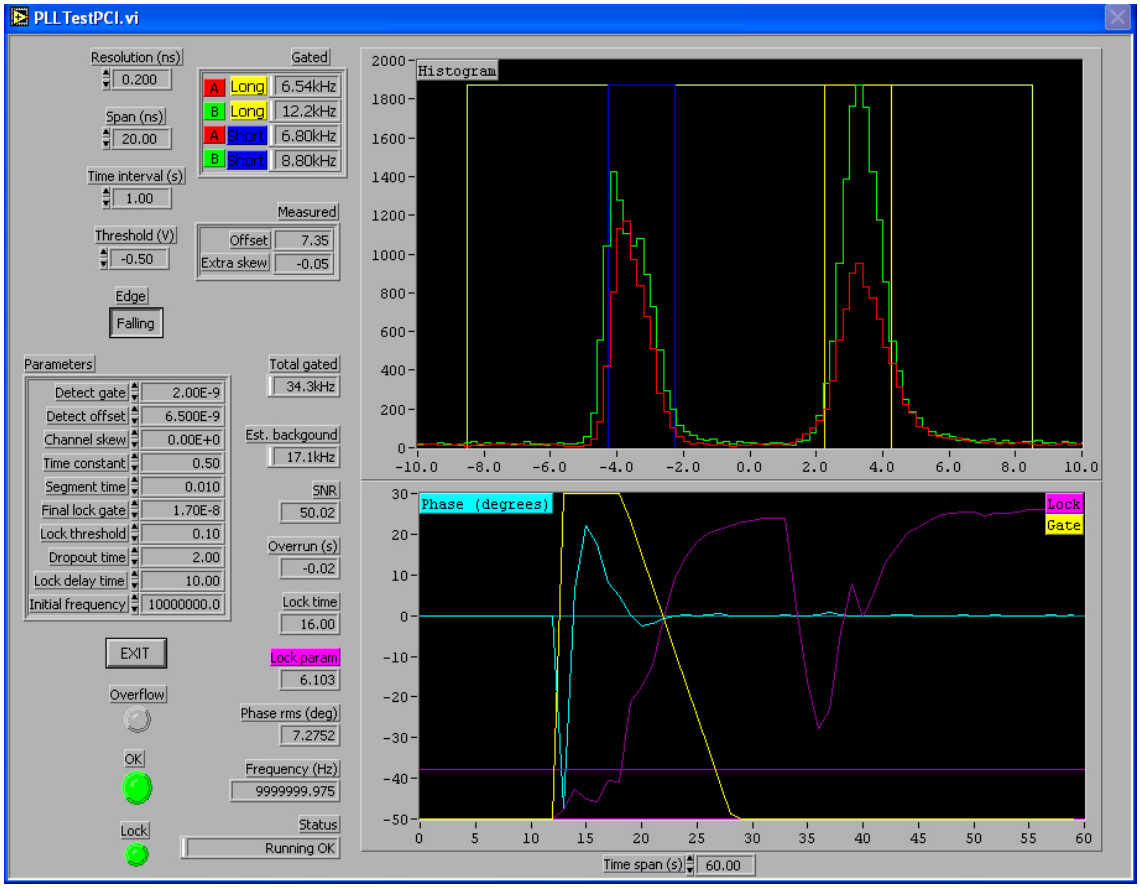


*Figure 5.6. Front panel of the PLLtest.exe program. A screenshot of a diagnostic program "PLLtest.VI". The top window shows four histograms (representing photon detections in the two channels) displayed in two 1.4ns timing gates separated by the delay line propagation duration. This system is locked (i.e. Alice and Bob are synchronised), as shown by the green marker at the bottom right of the frame.*

***Send Matrix.exe***

Automatically launches ReceiveMatrix on the Receive slave machine.

***ReceiveMatrix***

This is another program useful for system diagnostics. A fixed pattern modulation of the lasers is performed by the transmitter and the distribution of detected events is examined to allow correlation with the pattern sent. A matrix is produced of count rates in the receiver channels as they are distributed across the different bases. The detected events are sent with known polarisation and the distribution across the detectors is predictable in an ideal system.

This can help to diagnose potential problems with the alignment of polarisation either within the transmitter or relatively between Alice and Bob units. It will also show the relative intensities in each of the detectors. This program requires the total count rate to be less than 30KHz to operate.

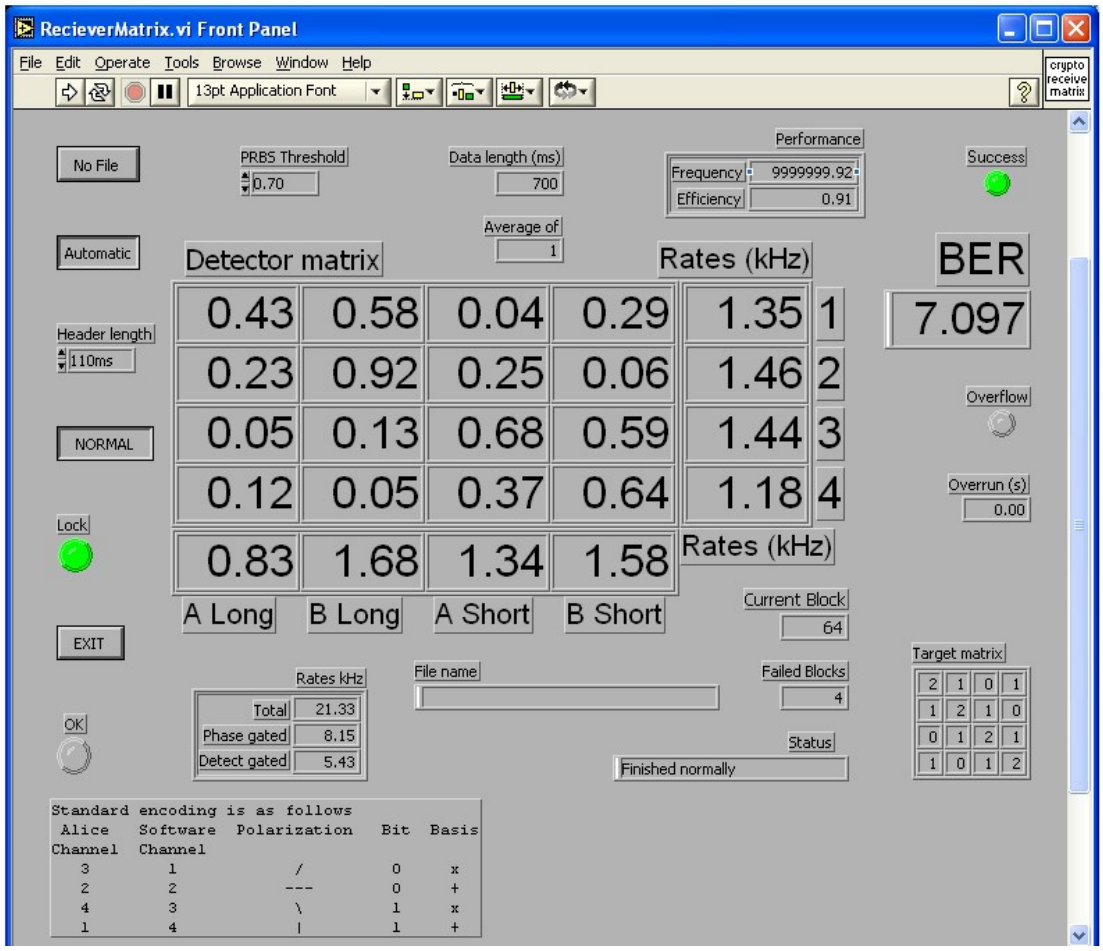


*Figure 5.7. A typical matrix generated by SendMatrix.EXE*

The four rates on the right hand side of the matrix should have similar values. These numbers show the total count rates received when each of the four Alice channels is being used with the other three channels off. A significant lack of balance here results in reduced security (it may or may not also degrade the QBER). If this happens it would be necessary to readjust the Alice channel intensities.

The matrix itself contains sixteen numbers but only eight of these contribute to the QBER. These are the leading diagonal (which should be as large a number as possible) and the second broken diagonal (the numbers showing 0.04, 0.06, 0.05, 0.05 in the screenshot). The broken diagonal numbers should be as small a possible to get a good QBER. Large numbers could indicate a polarisation or a signal to noise problem. This would either indicate a low signal level due to poor alignment, or a high background level due to excessive ambient light.

## 5.7 Experimentation and Trials

### *5.7.1 Laboratory tests*

In preliminary laboratory tests the system was shown to generate raw key data at rates up to 10kilobits per second (kbps) when simulating a 10dB transmission loss over the short transmission path and using a mean photon number, μ, of 0.1 photons per pulse. This suggests that the overall receiver efficiency was around 10%, although in the laboratory it was possible to achieve almost total absence of background light enabling the use of simple colour glass filters and multi-mode fibre coupling for the detectors.

The system error rates in the $45^0$ channel were initially found to be high (>10%). This was attributed to birefringence in the various transmitter recombining beamsplitters and was compensated for by using a single quarter wave plate in the receiving optics $45^0$ channel. The error rate was subsequently measured in each channel at approximately 2%.

| **Mean photon number (+/-5%)** | 0.01 | 0.0027 | 0.0008 |
|---|---|---|---|
| **Simulated loss (dB)** | 10 | 16 | 21 |
| **Raw key rate (Bits/s)** | 10000 | 1445 | 295 |
| **Sifted Key Rate (Bits/s)** | 5000 | 722 | 137 |
| **Corrected key rate. (Bits/s)** | 4500 | 432 | 76 |
| **Error rate (%)** | 2 | 3 | 6 |
| **Error correction efficiency (%)** | 90 | 61 | 55 |
| **Total key exchanged. (Bits)** | - | 23800 | 8320 |

*Table 5.2. Key exchange results from laboratory tests. The mean photon number here is the number arriving at Bob after the simulated loss (NB: The results show a non-linear relationship which is probably due to misalignment of the beam due to beam-shift introduced by multiple, thick neutral density filters).*

The initial key sift reduced the bit rate to ~5 kbps whilst the inclusion of error correction (at 2% error rate, roughly 90% efficient) yielded a final key exchange rate of order 4.5kbps. Using a 10Mbps Ethernet link between the two computers sifting and error correction were performed in real time. The results of the brief laboratory tests are shown in the table above.

### *5.7.2 1.2km Field test*

With the successful completion of Initial system tests in a laboratory environment, the system was moved to a dedicated optical testing facility located at a disused airfield near Pershore, Worcestershire, U.K. The facility consists of two compounds, equipped with optical laboratories (including stable optical tables) separated by a distance of 1.2km. The two laboratories were connected by a dedicated low speed (19.6kbps) microwave link for instrumentation purposes. An aerial view of the test facility is shown in Figure 5.8.

The receiver system was carefully shielded from any leaking light allowing the system performance in daylight to be tested. Using single mode fibres coupling the detectors to the telescope and 5nm bandwidth interference filters, dark count rates in bright, sunny conditions were measured at approximately 10kcps dropping to below 1kcps after dark.


*Figure 5.8. An aerial view of the initial system test site at a disused airfield near Pershore, Worcestershire, U.K. The transmission path was 1.2km (marked in red) along the side of a former runway with the two compounds connected by a microwave link.*

The transmitter was also shielded (to prevent light leakage from the transmitter laboratory from entering the distant receiver) and aligned on the receiver at a high power setting. Turning mirrors with fine manual micrometer adjustment were used for the alignment procedure.

During alignment a detector count-rate-meter sub-program allowed receiver photon counting rates to be monitored remotely at the transmitter. A screenshot of this diagnostic tool can be seen in Figure 5.9 below.

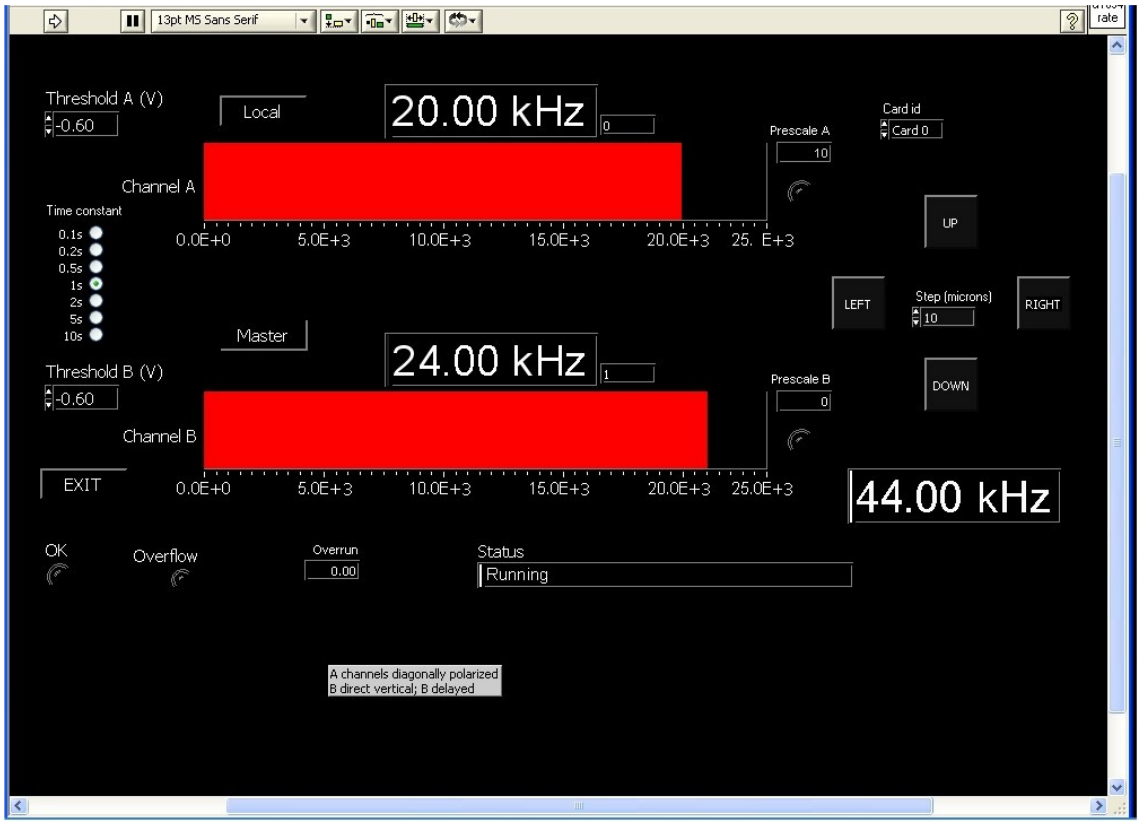


*Figure 5.9. A screenshot of the diagnostic program "Ratecounter". The program allows real time monitoring of receiver count rate at both remote and local terminals. This is very useful for alignment and testing.*

The beam was then attenuated and the collimation and fine alignment of the transmitter and receiver optics was optimised. It was clear at this stage that collimation of the transmitter beam was limited by turbulence induced beam wander. The minimum collimated beam diameter achievable at the receiver was of order one metre. For an example of the effects of turbulence over the same transmission path the reader is referred to chapter 3, figure 3.27.

Key exchanges were achieved at various optical powers down to 0.1 photons per pulse with full key sifting and error correction implemented over a serial link between transmitter and receiver computers. Key rates are summarised below in Table 5.3.

| **Mean photon number (+/-5%)** | 0.92 | 0.27 | 0.163 | 0.1 |
|---|---|---|---|---|
| **Raw key rate (Kbits/s)** | 2.22 | 1.08 | 0.55 | 0.35 |
| **Sifted Key Rate (Kbits/s)** | 1.098 | 532 | 270 | 173 |
| **Corrected key rate. (Bits/s)** | 367 | 256 | 104 | 18.2 |
| **Error rate (%)** | 5 | 6.4 | 7.5 | 11 |
| **Error correction efficiency (%)** | 33 | 48 | 38 | 10.5 |
| **Total key exchanged. (Bits)** | 3672 | 2559 | 2921 | 1442 |

*Table 5.3. Summary of results from the 1.2km system test. The test run culminated in a key exchange with a $\mu$ of 0.1 achieving a 18bps final key rate.*

With the classical channel bit rate limited to the 19.2kbps of the microwave link it was not possible to sift and error correct in real time as the key sift operation requires the timing data (a 32 bit integer) and measurement basis for each photon arrival to be sent from the receiver. (A transmission rate in excess of 70kbps would be required for real time sifting in this experiment).

Typically, key sifting could be performed at around 270 bits per second. Cascade error correction is much less data intensive and could operate at more than ten times this rate.

The main limitation to the experiment was found to be the high turbulence levels on the low level path and high error rates due to background counts. Higher order atmospheric effects such as scintillation and wavefront angle of arrival fluctuations were not considered to be a major problem over this short range and were not corrected for.

A second trial was planned over a 1.9km elevated (lower turbulence) path with improved background rejection in an attempt to alleviate these problems.

### *5.7.3 1.9km system trials*

For the second trial an elevated optical path from the laboratory (60m elevation) to a site on the side of the Malvern hills (260m elevation) was chosen in an effort to reduce the effects of turbulence. The optical beam was in excess of 30m above ground for most of this downwards slanting path which extended over 1.9km. The transmitter was located at the high end of this path looking down at the receiver. An aerial view of the experiment is shown in Figure 5.10.

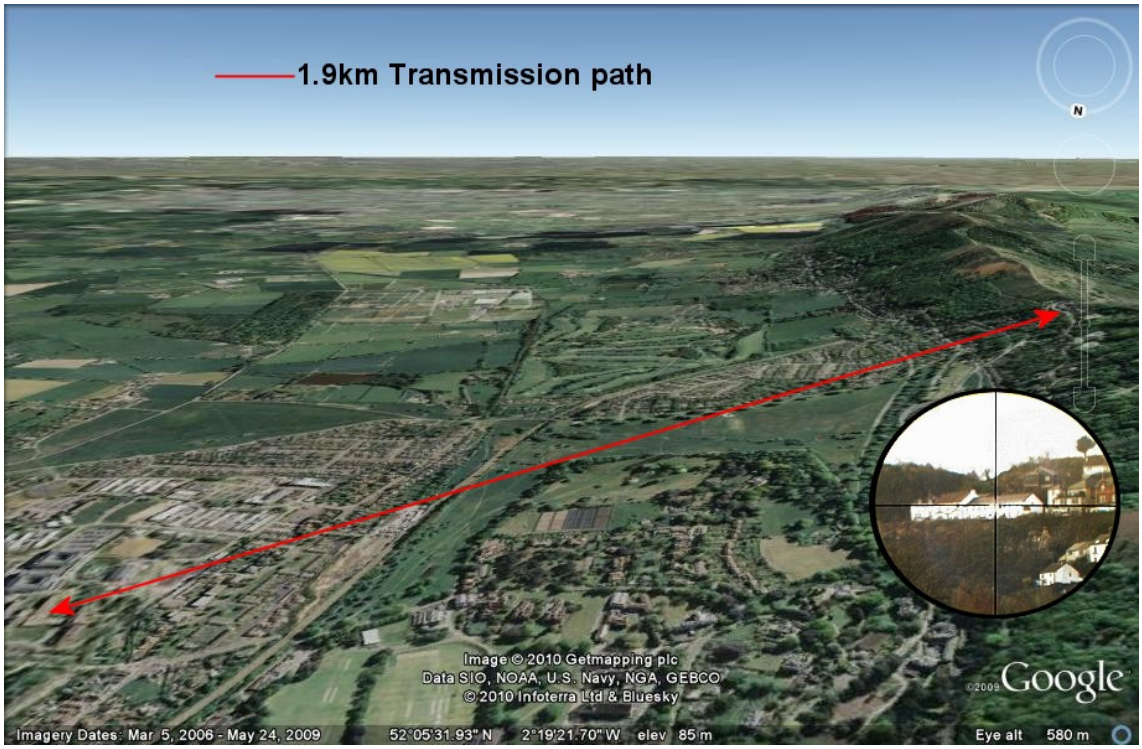


*Figure 5.10. An aerial photograph of the 1.9km transmission path. Most of the path was significantly (>30m) above the ground with the transmitter at the highest point, located in a public house (inset: telescopic view from the receiver location).*

By careful focussing the transmitter beam could be reduced to close to the diffraction limit (of order 0.12m). However, beam wander due to turbulence and transmitter pointing stability was still of order 20cm (100μradians) and it was found easier to work with the beam diameter closer to 0.5m to stabilise the counting rates. The background count rate was minimised by confining work to night hours only and blocking local stray light sources including street lamps. These precautions allowed the use of coloured glass filters and multimode fibres for detector coupling. Background rates of between 1 and 4kcps per detector were reached.

Trials operations proceeded in much the same way as for the 1.2km trials. The transmitter and receiver locations were linked by the public switched telephone network through computer modem cards with a typical bit rate between computers of approximately 33 kbps. This arrangement allowed raw key sifting at around 500 bits per second and distillation of error corrected key at around 1 kilobit per second.

| Mean photon number (+/-5%) | Raw key rate (Kbits/s) | Sifted Key Rate (Kbits/s) | Corrected key rate. (Bits/s) | Error rate (%) | Error correction efficiency (%) | Total key exchanged (Bits) |
|---|---|---|---|---|---|---|
| 0.76 | 3.8 | 1.9 | 954 | 6.48 | 51 | 21465 |
| 0.45 | 3.1 | 1.51 | 850 | 5.9 | 56 | 19045 |
| 0.39 | 2.55 | 1.27 | 651 | 6.2 | 51 | 14710 |
| 0.19 | 1.35 | 0.53 | 256 | 10.7 | 16 | 2559 |
| 0.16 | 1.11 | 0.57 | 304 | 6.44 | 54 | 13635 |
| 0.15 | 1.08 | 0.54 | 257 | 8.2 | 47 | 14197 |
| 0.39 | 2.49 | 1.24 | 685 | 5.1 | 55 | 15345 |
| 0.32 | 0.985 | 0.49 | 299 | 4.9 | 55 | 12992 |
| 0.126 | 0.574 | 0.28 | 162 | 6 | 57 | 8540 |
| 0.092 | 0.30 | 0.148 | 81 | 6.5 | 55 | 8116 |
| 0.081 | 0.25 | 0.123 | 71 | 5.65 | 57 | 6794 |

*Table 5.4. Summary of results from the 1.9km QKD trials during November 2000.*

Table 5.4 shows a selection of results taken during the trial at various values of μ. From the results shown the estimated effective transmission loss, L, is approximately 20dB for the range of experiments carried out. The transmission varies from experiment to experiment as a result of beam wander and varying collimation due to atmospheric turbulence.

### *5.7.4 The EQCSPOT long range system*[7]

With the intention of fulfilling a deliverable for work package three of the EQCSPOT programme (and as a project finale), a long distance trial of free-space technology developed in the programme was proposed. The teams involved in the trial were the DERA Malvern team from the U.K. and the Ludwig-Maximillians Universität team from Munich, Germany. The objective was the demonstration of at least a 10km key exchange using the miniaturised technology developed during the programme. The target transmission distance was chosen as it was in excess of the equivalent vertical path to a low earth orbit satellite thus demonstrating the preliminary feasibility of ground to satellite QKD.

In order to minimise the effects of turbulence the trials location was chosen over an elevated path between two mountains in Bavaria, southern Germany (within reasonable driving distance of the LMU campus). For the receiver location, a cable car station on the peak of Karwendelspitze was specified, whilst the transmitter was located at the Institute for Extraterrestrial Physics, a small experimental facility on the summit of Zugspitze, also reached via cable car. The distance separating these two locations was measured by GPS as approximately 23.4km, at the time, 2001, by far the longest attempted free-space transmission of QKD reported [10], [11].

### *5.7.5 Long range Alice*

The Alice transmitter was built on a 300×600mm optical breadboard incorporating a novel miniature Munich-built transmitter module in a folded optical path. The source was expanded and then collimated with a simple telescope (100mm output lens) to a beam diameter of approximately 50mm. Whilst the output wavelength was specified as 850nm a tracking laser was included operating at 635nm, sufficiently spectrally separated from the Alice source to avoid crosstalk noise. The transmitter was equipped with a Perspex cover for protection with the whole system mounted on a heavy tripod. A tracking camera was slung beneath the breadboard as an alignment aid. The first iteration of the transmitter may be seen below in Figure 5.11

[7] This effort was a collaboration between the LMU and DERA teams. The author was responsible for the Alice optical system (not the actual emitter) and tracking camera, Alice interface electronics and trials organisation for the U.K. team.

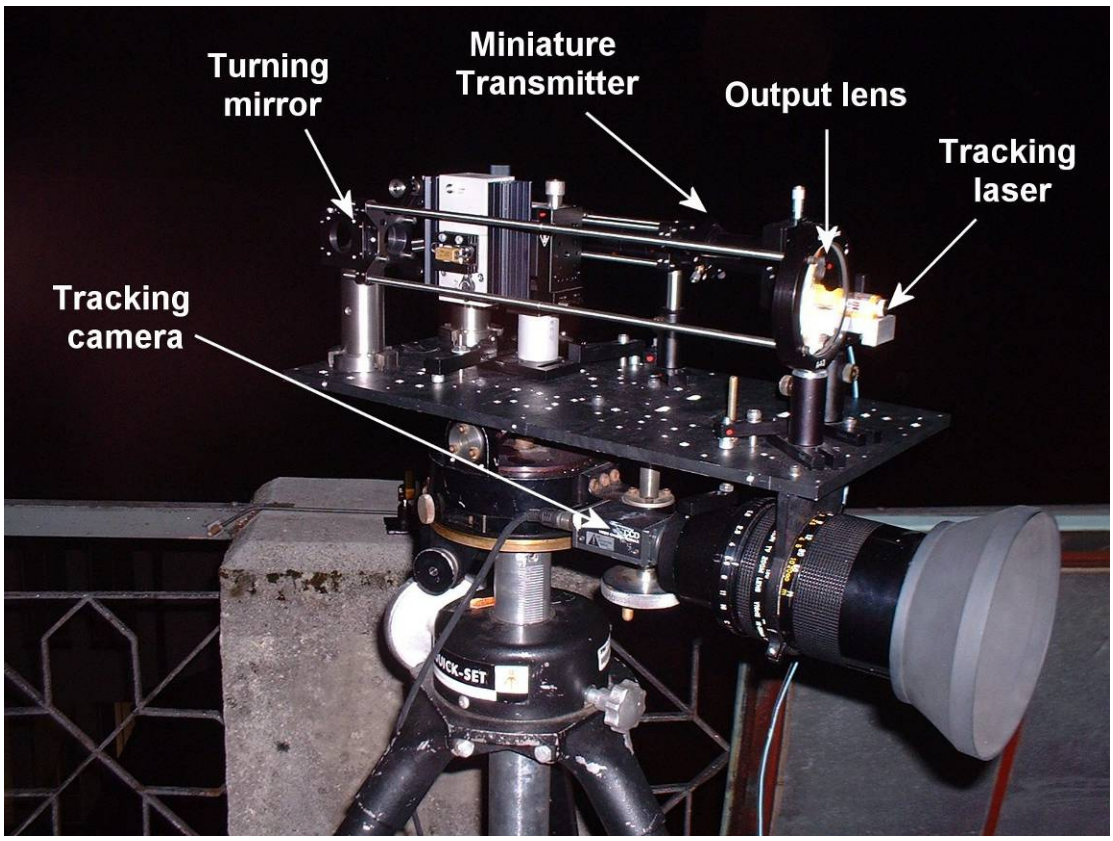


*Figure 5.11. Photograph of the initial long distance Alice transmitter. During the trials several improvements, such as pointing accuracy, were made based on practical experience.*

Initial problems with pointing accuracy led to the system being remounted on a micro-radian sensitive pointing stage. In common with previous EQCSPOT free-space systems the Alice module was driven at 10MHz to produce pulses randomly polarised in 0, 90, 45 or 135 degree polarisation directions.

### *5.7.6 Long range Bob*

The Bob system consisted of a 30cm diameter commercial Schmidt-Cassegrain telescope (Meade LX200) with computer controlled pointing capability. The telescope output was coupled to a “flip” mirror allowing two output ports. The first port was used to mount an adapted version of the Munich compact photon counting detector module (similar to the generic Bob discussed in chapter 4), whilst the second port was coupled to a CMOS camera used for tracking purposes. The telescope barrel was adapted to mount a low power 532nm tracking laser and the whole system was mounted on a Meade proprietary tripod. A photograph of the Bob system is shown below.

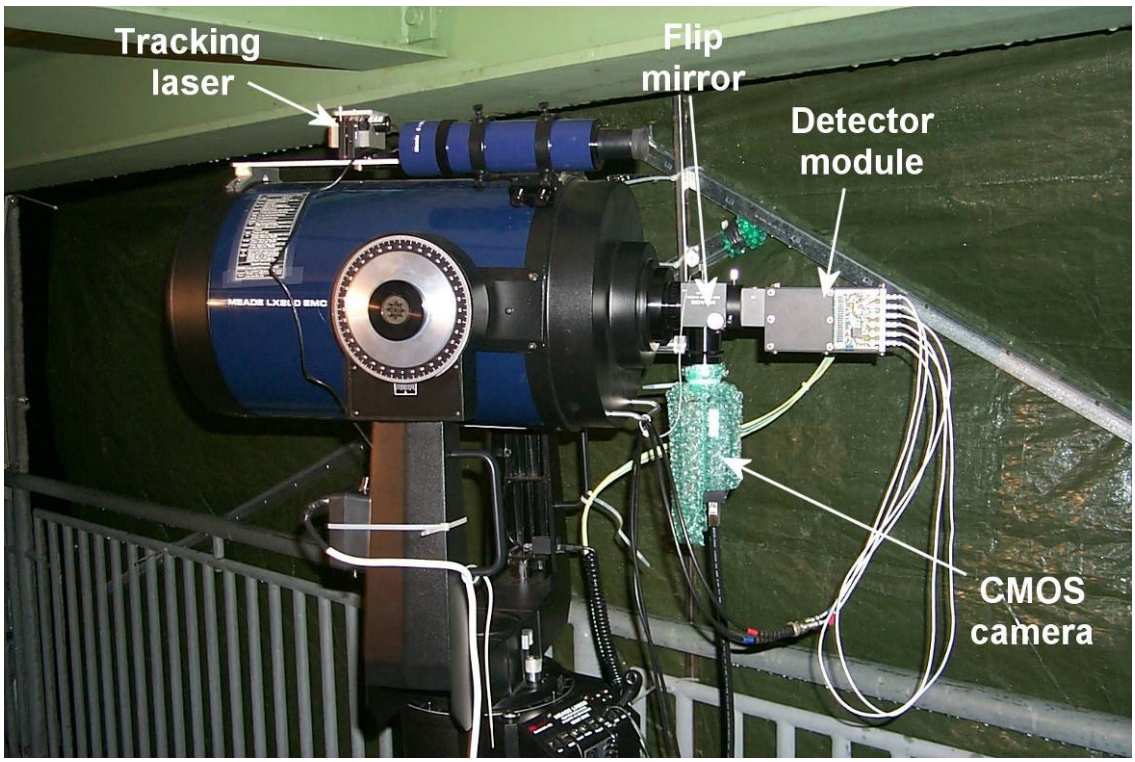


*Figure 5.12. The Bob optical system seen in-situ at the cable car station on Karwendelspitze. Essential components required lagging due to the exceptional cold at the altitude and time of year.*

### *5.7.7 Trials operations and results*

Due to the inclusion of versatile interface electronics and systems, it was possible to use the controlling computers, complete with software and diagnosis programs, from the previous U.K. trials.

Coarse alignment was achieved by directing a low power alignment laser from each end in turn and adjusting the tripods iteratively. Fine alignment was then performed by switching off the alignment lasers and substituting an alignment source designed to emit through the pinhole of the spatial filter of Alice. Once aligned the system was tweaked using the data sources

The collimation in the Alice system was such that at 23.4km the beam was 1-2 metres in diameter. This led to lumped optical losses of about 18-20dB. With a receiver efficiency of around 15% and using faint pulses containing 0.1 photons per bit the detected bit rate at Bob was about 1.5-2kbps. Sifting and error correction were then performed over a standard mobile telephone link equipped with software modems and G.S.M data capability.

Early in the trials an optical free-space link was implemented via a separate channel and was used for voice over IP (VOIP) and data exchange. Unfortunately, alignment issues over these long haul channels were such that that without active tracking the system was untenable.

A selection of successful key exchange results from the trials are shown below in Table 5.5.

| **Number of photons per bit (+/-5%)** | 0.37 | 0.27 | 0.18 | 0.096 | 0.081 |
|---|---|---|---|---|---|
| **Raw key rate (bps)** | 4484 | 2505 | 2651 | 2627 | 2127 |
| **Background (bps)** | 6268 | 5504 | 5578 | 4516 | 4474 |
| **Error rate (%)** | 4.11 (1.96) | 5.24 (3.08) | 4.54 (2.94) | 4.77 (2.41) | 5.81 (2.94) |
| **Error correction efficiency (%)** | 51 | 56 | 51 | 56 | 49 |
| **Final key rate (bps)** | 626 | 396 | 363 | 367 | 246 |
| **Total exchanged Bits** | 9395 | 4341 | 5448 | 5399 | 3799 |

*Table 5.5. Key exchange results from the trials at the Bavarian Alps in the winter of 2001. Error rates in brackets result from the contribution of the background.*

Background count rates were considered high for this experiment due to the optical scatter from the snow covered trials locations and the use of coloured glass filters in the receiver optics (Schott RG780). As a result, a large part of the error rate can be attributed to the elevated background count. The remaining error rate resulted from errors in the polarisation due to imperfections in the optical system. As seen above the error correction efficiency at these error rates is approximately 50%. Overall the efficiency of the key reconciliation process is approximately 16% with a factor of 0.5 lost in the initial key sift, close to 0.5 lost in the error correction and finally a factor of ~0.33 lost due to the efficiency of the data block method of transmission.

### *5.7.8 Discussion of trials results*

Key exchanges were achieved in all of the trials with varying degrees of success showing that free-space QKD is a viable technology even over several tens of kilometres. All of the experiments produced sifted and error corrected final keys as part of the complete system implementation. An informative figure of merit for QKD schemes is the quantum bit error rate (QBER). Below, the QBER is plotted against the the error correction efficiency using the data measured in the full set of trials presented above. For comparison the data is set against the Shannon limit for error correcting codes and the Tančevski estimate for the Cascade error correcting algorithm.

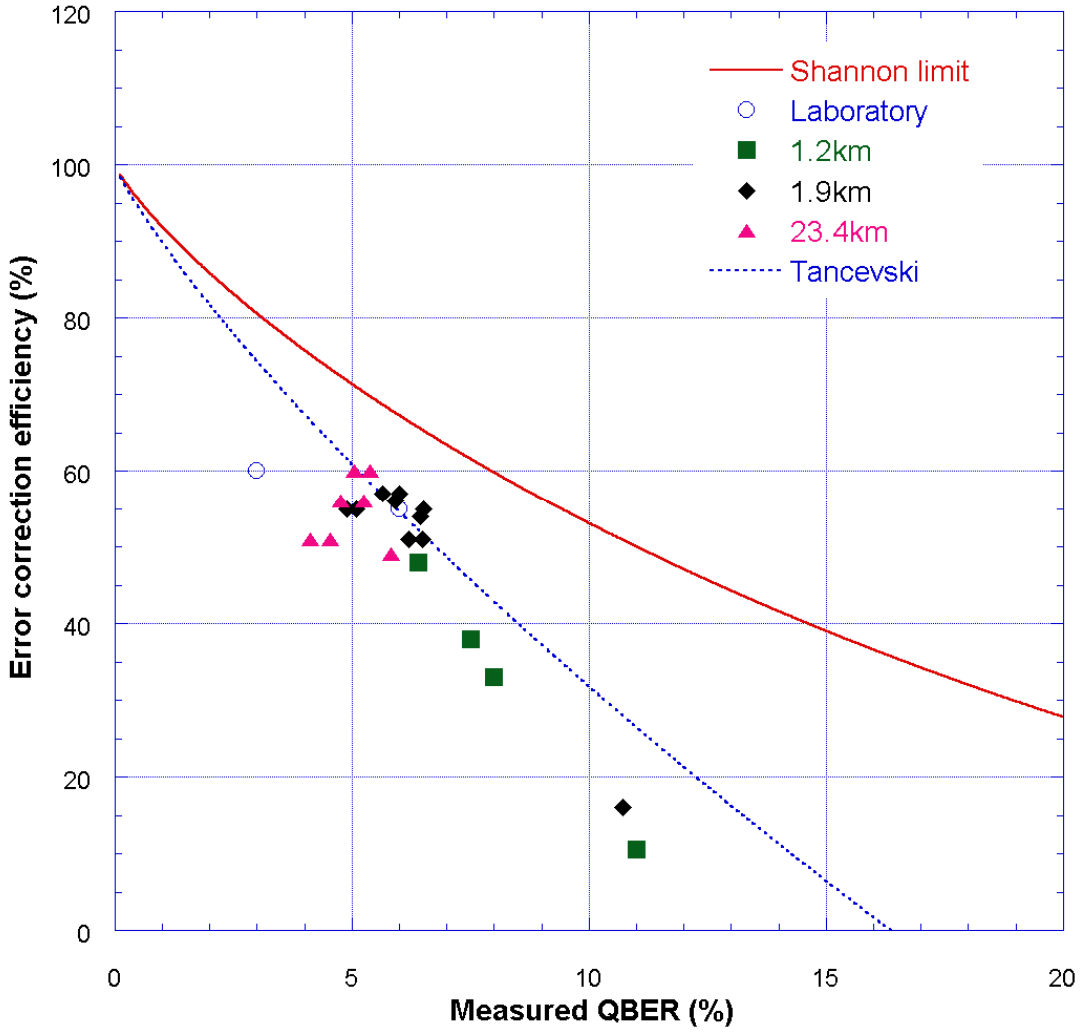


*Figure 5.13. Error correction efficiency plotted against measured Quantum bit error rate for the experimental data shown in tables 2-5 above. Also plotted is the theoretical maximum efficiency (Shannon limit) and the estimated efficiency of Cascade (after Tančevski et al).*

The reason for using error correction efficiency as a figure of merit is that at the time of these experiments there were no robust security analyses available for operating QKD systems, thus a convenient measure of the efficiency of secure key generation of the system is to compare it with the theoretical best cases (i.e. Shannon and, in the case of the Cascade algorithm, Tančevski et al). In the graph above, the Shannon limit and the Tančevski estimate could be regarded as analogous to the idea of "gain" introduced by Lütkenhaus and developed further by other researchers such as Gottesmann, Lo and Preskill (see chapter 3, section 3.3.3-3.4.3).

Clearly the implemented error correction routine approaches the Tančevski limit when dealing with errors around 5%. Error correction of keys with greater than 10% error is extremely inefficient. At low error rates the cascade method has to reveal and discard a minimum amount of information (~30%) to check for errors and estimate an error rate. For this reason longer key strings are advantageous and would tend to exhibit better correction efficiencies.

Another factor to be considered is the development of the system itself. By the end of EQCSPOT the complete system was operating over ranges an order of magnitude greater than at the start. Furthermore, system size had decreased by at least a factor of two with the coupling telescopes being the largest components. In addition the practical experience gained was to prove invaluable for future system and software design.

## 5.8 Conclusion

This chapter has documented the author's involvement in the early development of free-space QKD systems from 1996 to 2001. The work included the construction of complete demonstrator system hardware and electronics for the European EQCSPOT collaboration. This work took place against the background of very little prior art of system construction. Several key exchanges were made over varying distances, culminating in a world leading transmission distance, at the time, of 1.9km (even reported in the national press at the time [12]).

Elements of the system were used later in a collaboration with Ludwig-Maximillians Universität, Munich achieving another record of a 23.4km transmission distance.

The mountaintop experiment described above effectively marks the end of the first decade of development of free-space QKD systems. The period was characterised by constant development and miniaturisation of system components as well as software refinement leading to extension of key exchange range (from 30cm to 23km) and moving QKD systems out of the laboratory and into the real world.

## 5.9 Chapter 5 references


[1] A. K. Ekert, J. G. Rarity, P. R. Tapster & G. M. Palma, "Practical quantum cryptography based on two-photon interferometry", Phys. Rev. Lett. **69**, 1293–1295, (1992).

[2] C. H. Bennett, and G. Brassard, "Quantum cryptography: Public key cryptography and coin tossing", Proceedings of the International conference on computers, systems and signal processing, Bangalore, India. December 1984. pp. 175 – 179, (1984).

[3] J. G. Rarity, P. R. Tapster, and P. M. Gorman, "Free-space key exchange to 1.9 km and beyond", J. Mod. Opt. **48**, 1887–1901, (2001).

[4] PicoQuant Picosecond laser diode heads datasheet, (2009).

[5] J. G. Rarity, P. R. Tapster, and P. M. Gorman, "Secure key exchange over 1.9 km free-space range using quantum cryptography", Electronics Letters, **37**, 8, 512-513, (2001).

[6] Perkin-Elmer single photon counting modules datasheet (2010).

[7] Adlink NudaQ PCI7300a High speed Digital Input/Output card datasheet, (2009).

[8] J. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, C. J. Williams, E. W. Hagley, and J. Wen, "Quantum key distribution with 1.25 Gbps clock synchronization", Optics Express **12**, 2011–2016, (2004).

[9] R. J Hughes, J. E Nordholt, D. Derkacs and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night", New Journal of Physics **4**, 43.1–43.14, (2002).

[10] C. Kurtsiefer, P. Zarda, M. Halder, P.M. Gorman, P.R. Tapster, J.G. Rarity and H. Weinfurter, "Quantum cryptography: A step towards global key distribution", Nature **419**, 450, (2002).

[11] C. Kurtsiefer, P. Zarda, M. Halder, P.M. Gorman, P.R. Tapster, J.G. Rarity and H. Weinfurter, "Long distance free space quantum cryptography", Proc. SPIE Vol. 4917, 25-31, Quantum Optics in Computing and Communications, (2002).

[12] "Will they put the spies out of work?", The London Daily Telegraph, 9/10/2002, p20.

# Chapter 6 – Research and Development work, 2002-2006

## 6.1 Introduction

In the previous chapter, the design, build and testing of a primitive free-space QKD system was described, culminating in a 23.4km range QKD experiment in the mountains of southern Germany in 2000.

At this time several similar (from the point of view of maturity) systems were being tested in almost real world scenarios. However, like any new technology application, the systems were bulky, heavy, power-hungry and unstable, requiring much attention from highly skilled operators. The next phase in QKD research was to see concentration on sub-system design such as single photon counting systems, random number generators and miniaturisation of QKD components. This chapter will review this developmental phase, in terms of research and development of free-space QKD at QinetiQ.

## 6.2 QKD development at QinetiQ

With the end of EQCSPOT, QKD research at QinetiQ continued under the auspices of several collaborative programs, namely QUCOMM (Long distance photonic Quantum communication), ICQKD (Intercontinental QKD) and ESA-QSPACE (Quantum communications in space). In mid-2004, the team at QinetiQ also received funding from the UKMoD basic research programme to develop free space QKD technologies.

Part of the way into the project, a proposal was received from BBN Technologies of Boston, Massachusetts, with the intent of acquiring a free-space QKD node for inclusion in the DARPA quantum network, a metropolitan test bed for quantum cryptography [1].

As a result of these funding sources, the main focus of QKD research at QinetiQ during this period was:-

- Random number generator suitable for QKD use.
- Development of compact QKD transmitter technology.
- Development of compact QKD receiver technology.
- Software and algorithms.
- Demonstrations and long range trials of components.

Each of these areas will be discussed in turn with a description of some of the tests and trials conducted to validate system designs.

## 6.3 Random number generator development[8]

Random numbers are at the heart of a QKD system. The selection of the output polarisation state of the Alice transmitter must be random [2] so it is important to be able to acquire high speed, high quality random numbers in order to make that selection. Previous QKD experiments, for the most part, either used a pseudo-random file stored on a computer hard drive [3] or a white noise source [4] to generate the random numbers for switching Alice. The former approach lacks the required randomness whilst the latter tended to be slow. The object of this work was to produce a robust source of random numbers with several properties:

- Simple construction and low cost.
- Minimum random bit rate of 10Mbit/sec.
- High quality randomness.

The method chosen was that based on the amplification of electronic noise in a transistor amplifier. The reasons for this choice was that this type of noise source was easy to implement and provided a well-known, scalable method of noise generation.

## 6.4 Prototype RNG

To achieve the design goals, a simple circuit was designed using LM733 differential amplifier integrated circuits in a twin channel, three amplifier cascade configuration. The design featured amplifiers with a gain of approximately 100 and included an adjustable attenuator placed between each stage. Overall, each channel was designed to produce a voltage gain of approximately $10^5$. Thus noise present in the first IC was amplified by the subsequent ICs to generate an analogue noise voltage of approximately 500mV RMS amplitude. The spectrum was reasonably flat in the frequency range 10kHz to 20MHz with the overall amplifier bandwidth measured at approximately 50MHz.

This white noise was then added to a DC voltage level and fed to a buffer amplifier (Texas Instruments BUF634 amplifier). The two channels of analogue noise were then connected to two of the input bits of a 32 bit digital I/O card in a PC. The I/O card was set to perform a thresholding operation, recording a 1 when the analogue voltage exceeds some threshold and a 0 bit otherwise.

[8] This work was conducted in collaboration with Paul Tapster. The author was mainly responsible for the hardware design and fabrication whilst PT was largely responsible for software and testing.

The mean DC level delivered by the analogue stage was adjusted to ensure that the probability of the digital levels being 1 and 0 are as close as possible to 50% each. A schematic of the circuit is shown in Figure 6.1

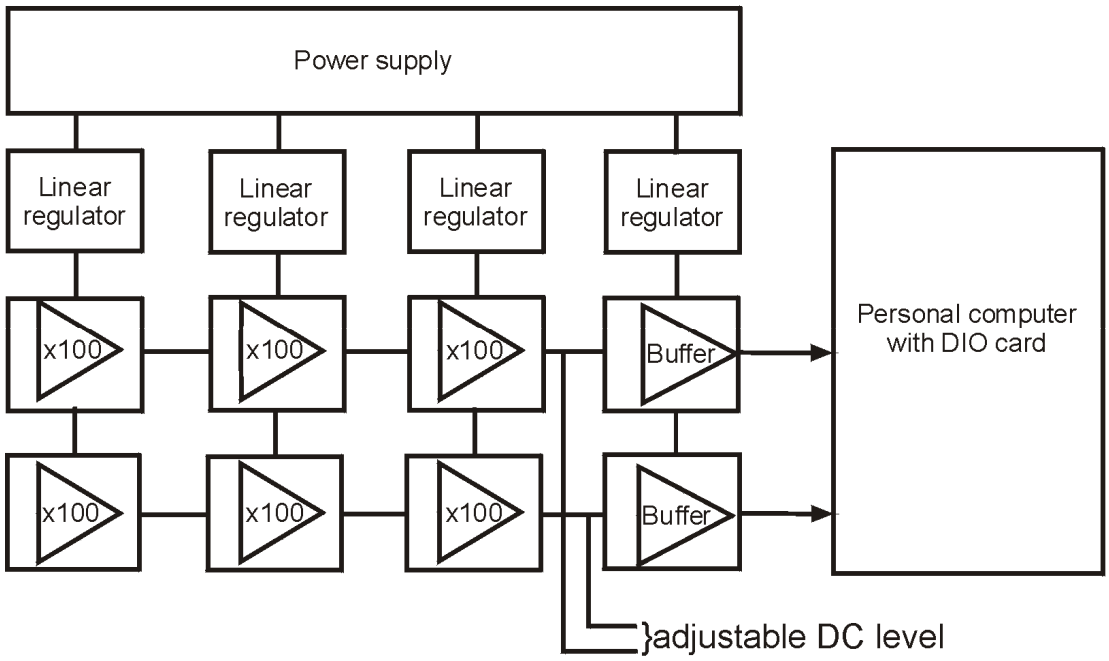


*Figure 6.1. Schematic of the prototype random number generator. The noise source consisted of a twin channel amplifier cascade with the output being sampled by a DIO card resident in a PC. A DC voltage source was fed to each channel allowing the mean voltage level of each channel to be adjusted.*

In the design and construction of the circuit, care was taken to avoid positive feedback (which could have led to oscillation of the circuit). Power supply decoupling was achieved with the use of multiple value capacitors at every component with power being supplied by several linear regulators. The RNG output was fed to the input ports of the DIO card using high quality shielded cable. The digital IO card was programmed to sample its inputs at various rates and transfer them to the PC memory. Once loaded into the computer memory various operations were performed to verify and, if necessary, increase the randomness of the bit stream.

In the first instance an exclusive-OR function was used (on non-temporally adjacent bits) which is known to have the effect of decreasing the bias of the random bit stream. An optional compression stage was also added, allowing the quality of the random bits to be improved almost arbitrarily at the cost of bit rate.

A suitable compression algorithm was used to convert the 20MBit/sec raw data to 10MBit/sec. The deviations from ideal random bits were then barely detectable.

## 6.5 Brassboard RNG

Whilst the performance of the prototype RNG was satisfactory, further development was proposed with the goal of improving noise performance and random bit rate. The opportunity was also taken to improve the utility of the device for QKD purposes. To this end an improved design was produced incorporating several improvements to the original. These are listed below:-

- Better amplifier circuit, including gain shaping, leading to a wider bandwidth allowing a greater sampling rate of the noise.
- Double the amount of amplifier channels allowing sampling across 4 input bits of the DIO card thereby doubling the random number yield.
- Automatic bias adjustment. The random numbers were continuously sampled and tested. Any variation of bias resulted in an error signal fed to an onboard 4-channel 12-bit DAC allowing continuous adjustment of the DC offset voltage (and thus the output bias).
- Industry standard PCI form factor. This allowed the RNG card to be plugged directly into the PCI bus of the Alice PC and would allow the use of multiple cards in a single PC.
- Redesigned power supply. Power was drawn from the computer PCI bus and conditioned by several DC-DC converters, each feeding a linear regulator (one for each amplifier stage). The DC-DC converters were synchronised such that their switching frequencies were identical. (The “sync switches” in the photograph were included for testing the effects, if any, of loss of converter synchronisation).
- Use of HF construction techniques and a metal screened enclosure for the amplifier circuit to provide protection from electro-magnetic interference, both incoming and outgoing.
- Professional PCB manufacturing techniques with the use of ground and power planes and effective power supply decoupling.

The final realisation of the card can be seen in Figure 6.2.

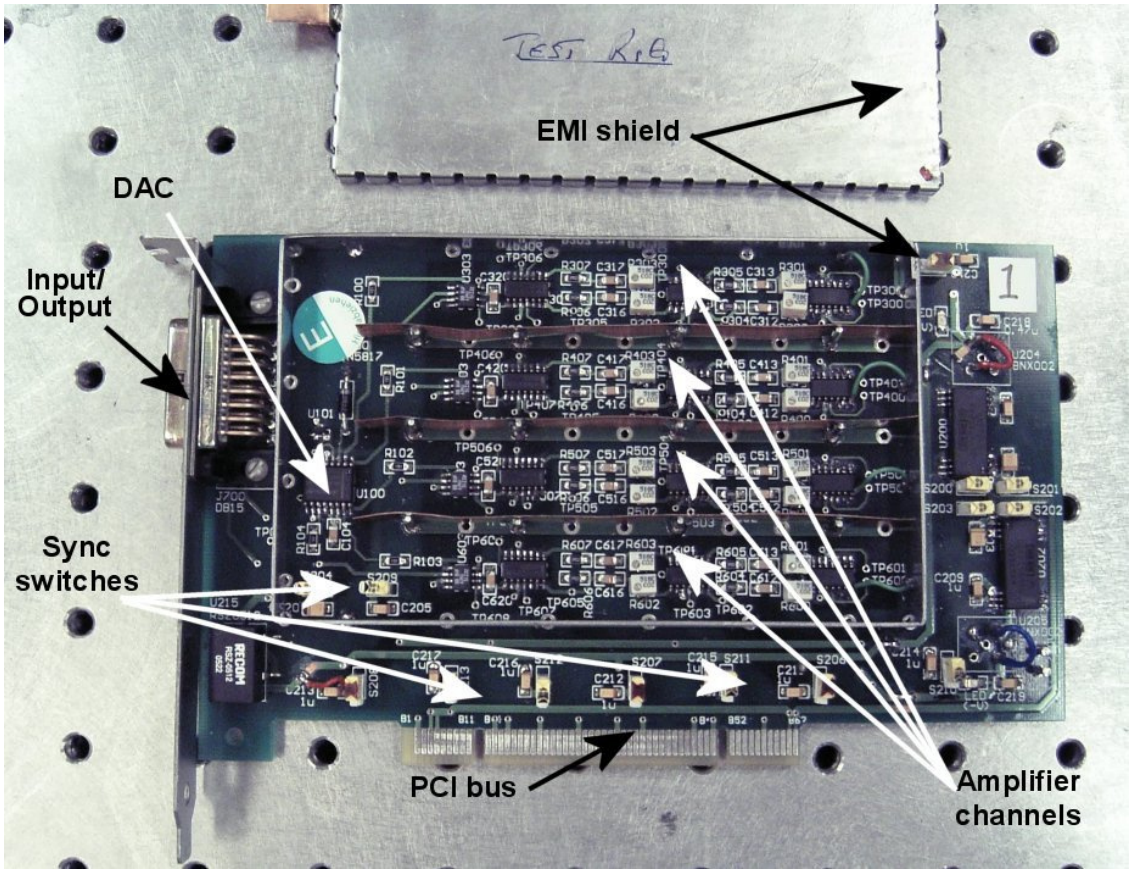


*Figure 6.2. The brassboard PCI random number generator with EMI enclosure opened to show the four amplifier channels.*

### 6.6 RNG testing

A measure of all deviations can be summarised by the Shannon Entropy, which is a measure of the information content of the random bits [5]. The measured Shannon Entropy of this system was 98% of the ideal value, however, measurement of the entropy of the device is not generally considered sufficient to guarantee high quality randomness.

In light of this the RNG described above was subjected to the tests detailed in both the FIPS 140 standard [6] and the Diehard suite [7].

### 6.7 General RNG performance

The set of graphs below depict the frequency spectrum and autocorrelation functions of the output of the RNG. The random bit generator showed extremely small deviations from perfection.

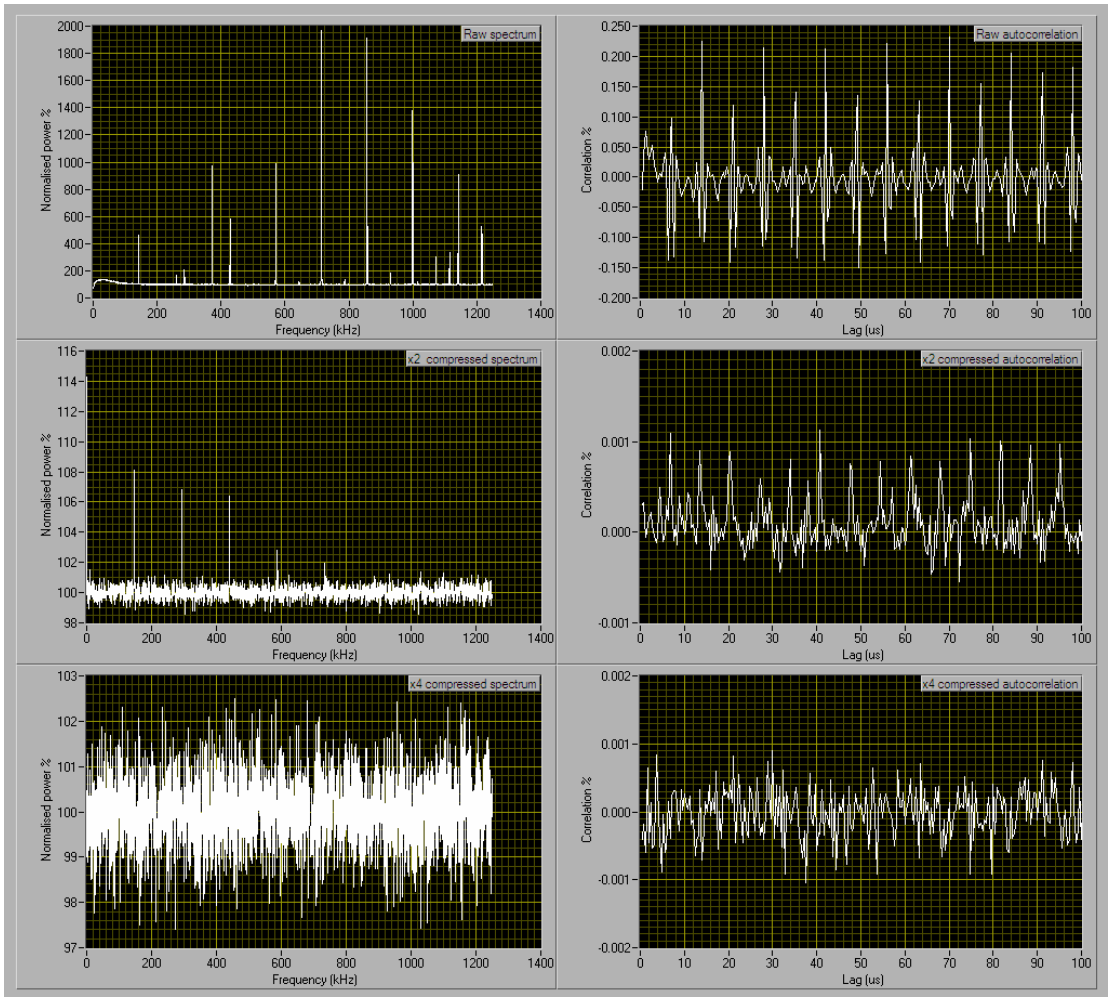


*Figure 6.3. Graphs showing the noise generated by one of the RNG cards in terms of the normalised power spectrum and the autocorrelation of the sampled bits. Three sets of results are plotted for the raw data: top with sampling at 80Mbit/s, middle with compression to 40Mbit/s, and bottom with compression to 20Mbit/s.*

Figure 6.3 above (top right) shows the autocorrelation plot from the raw output of one of the RNG cards delivering 80 Mbit/s. The regular pattern of spikes is due to unwanted coupling from the electronic power supply into the random output channels. Careful design of the power supply reduced this effect to less than 0.25% but did not eliminate it. The graph at the top left of the figure shows the same information in the frequency domain, where a set of harmonics of the 140 kHz spurious signal are easily seen. By using software compression of the raw card output these artefacts can be reduced or effectively eliminated. The two diagrams in the middle row of Figure 6.3 show the effect of compression by a factor of two, reducing the output rate to 40 Mbit/s. There is more than two orders of magnitude reduction in the size of the effects, and the autocorrelation is now less than 0.001%.

The compact QKD system currently requires 20Mbit/s from the random number generator for real time operation, and so a factor of four was used to compress the data. With this compression it was no longer possible to find any deviations from perfect performance with the samples of $10^{10}$ bits used for these data. The lower two plots show the quality of the random number generator in the ×4 compressed mode. The regular peaks indicating deviations from perfect performance have now disappeared, and the horizontal noisy line appearing in both plots merely shows the statistical fluctuations inevitable whenever a finite sample of random bits is analysed.

The actual deviations, as measured by the correlations, must be accepted as arbitrary in the absence of any *robust* published standards. Probably the most used published standards in the community are FIPS 140 and the Diehard suite, of which the Diehard tests are the most constraining. It was found that the output of the RNG could pass the FIPS 140-1 tests without using any post processing (such as the XOR method), however, this was when the device was fully warmed up and operating at an ambient temperature close to that at which it was last adjusted. To demonstrate a more robust behaviour, the FIPS 140-1 tests were also run on the software compensated RNG output.

It was found the RNG passed the tests from cold and over a wide range of temperatures. To simulate the degradation in performance expected when operating the system over a wide temperature range, the bias adjustments were deliberately offset to make the probability of 1's in the raw output 55%. Then an eight Gigabit random number file was created by running the system for 20 minutes with the software compensation algorithm in use. Since the tests specified in FIPS 140 require only 20,000 bits, all the tests were repeated 400,000 times thus using all the bits in the file. The result of this was that one of the tests (the runs test) failed on one occasion, and all the other tests were passed.

This outcome is expected, since in the nature of statistical tests an ideal random number generator is expected to fail on rare occasions. This is because even a true random number generator will sometimes generate sequences which *appear* to be non-random. The randomness of the RNG described above is thus perfect as far as these tests are concerned.

The data with ×2 compression passed the Diehard tests but it was obvious that artefacts still remained when using our own correlation test. Therefore the RNG system was used with ×4 compression in the absence of any guidance from published standards.

### *6.7.1 RNG speed*

Using a PC running a 400MHz Pentium II processor, the rate at which raw random bits could be generated and saved to a data file was found to be $2.64\times10^7$ bits per second. Although the DIO card was sampling 4 bits at a rate of $10^7$ samples per second, the overheads associated with formatting the data, transferring it to the PC memory and then writing it to the hard disk reduced the data rate to 65% of the theoretical maximum. Later tests conducted using a 1.7GHz PC allowed a bit rate of $3.73\times10^7$ bits per second to be achieved. As noted above, if the XOR based compensation scheme is used the bit rate of the RNG is roughly halved. It was found that the Pentium II was able to produce essentially perfect random bits at a rate of $1.44\times10^7$ bits per second, whilst the 1.7GHz PC provided a bit generation rate of $2.00\times10^7$ bits per second (i.e. 20Mb/s). A patent application is pending for the implementation of the random number generator and its development [8].

As far as the author is aware these bit rates compare favourably with all hardware based random number generators reported to date. For example see [9], [10] & [11].

## 6.8 Development of a compact QKD transmitter[9]

Previously, a prototype Alice system was described which featured a commercial pulsed laser source combined with acousto-optic beam switching to generate the optical pulses. In addition, the electronic drive circuitry was built from a mixture of discrete components and 7400 series TTL integrated circuits mounted on standard Vero-board. Power was supplied from standard laboratory type power supplies. Whilst this arrangement was satisfactory for a demonstrator, the system was cumbersome, inefficient and fundamentally limited in switching speeds by the response of the acousto-optic modulators (<25MHz) and the bandwidth of the electronics (~50MHz for TTL logic).

A new approach was proposed whereby the Alice transmitter would be redesigned to operate with four, individually pulsed, laser diode sources coupled to a miniature optical system and housed inside a compact module. The system was to incorporate several improvements identified in the light of the trials experience gained by the team.

The approach effectively called for a completely new design of a compact QKD transmitter in which the following elements were considered:

[9]This work was conducted within a team environment. The author was responsible for design and fabrication of all Alice electronics, cabling, termination design and *initial* design of the optical system. Of course, all four team members had their own responsibilities but also at least some input to all other parts of the programme.

- Fast pulse generator – creation of a simple, fast, cost effective pulse generator suitable for pulsing laser diodes.
- Alice driver PCB – Design of a single circuit board containing all the necessary components to operate an Alice transmitter.
- Miniature optical bench design – complete with adjustable mountings for laser diodes and optics.

### *6.8.1 Fast pulse generator*

In a well designed optical system the main source of noise is background radiation, that is, stray radiation entering the detectors and creating erroneous data counts.

A useful method of achieving a reduction in background noise is to electronically "gate" the photon detectors. To do this, an electronic gate is opened when incoming light pulses are expected, and closed again as soon as possible thereafter. Thus, only light (signal and background) arriving over the duration of the gate is admitted to the photon counting system.

Clearly then, the shorter the gate, the smaller the amount of noise admitted to the system (up to a point, since once the gate becomes too narrow, signal loss begins to occur), provided that the transmitter can emit pulses which can fit inside the gate and both transmitter and receiver can be synchronised with sufficient precision. For this reason, a simple circuit was designed with the intention of generating short laser pulses (~1ns) at medium to high frequencies (10-100MHz). There are several methods known to produce pulses suitable for pulsing semiconductor lasers. Initially, the method of pulse generation investigated was that of creating avalanche breakdown in suitable transistors (for instance the 2N2222 NPN transistor). This is a well-known method and experimental circuits produced perfectly adequate pulses (see, for instance, [12]). The main disadvantages of this technique were the high voltages required to initiate the avalanche process (<200V) and the breakdown process itself which tended to induce crosstalk amongst the four channels when implemented in test circuits. An alternative method was then investigated in which a pulse is generated by propagating a suitable transient through a delay line differentiator such as that described in [13].

#### *6.8.1.1 Delay line pulse generator*

The delay line based pulse generator is not a new idea, however, with modern components and fabrication techniques, the capabilities of these circuits are tremendous. For instance, pulse widths as short as a few hundred picoseconds have been reported

[14] by using the latest step recovery diodes (see [15] for an excellent discussion of SRDs and their applications) and circuit design.

The pulse generator uses a step recovery diode (SRD) coupled to a shorted delay line to generate a fast pulse. The generator function is explained below:

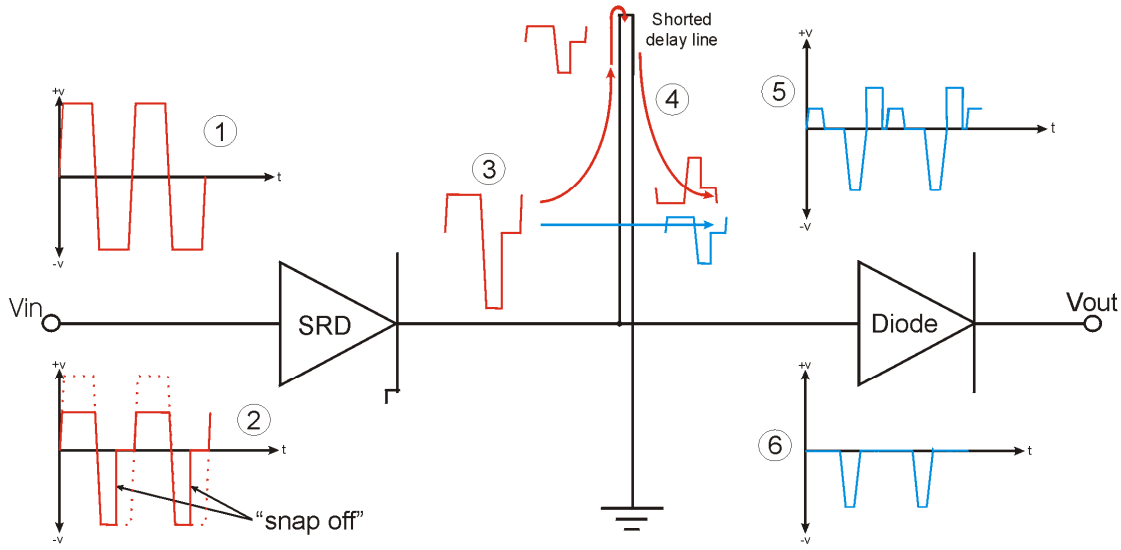


*Figure 6.4. Diagram showing operation of the step recovery diode – delay line pulse generator.*

With reference to Figure 6.4 above the operation of the generator proceeds as follows:-

1. A square wave drive signal is applied to the input of the pulse generator.
2. Whilst forward biased during the positive half cycle of the drive signal the SRD conducts as normal. However, as the drive signal enters its negative half cycle, the diode continues to conduct as the stored charge is removed from the junction region of the device. This process occurs slowly in normal diodes, but in SRDs the junction region is engineered to remove this charge abruptly, thus creating an abrupt conductance change. This abrupt change is commonly called "snap-off" and is shown in Figure 6.5 below.
3. An abrupt change in current in the SRD produces an abrupt change in voltage across the load. This abrupt change travels to the shorted length of delay. This transition is then split between the transmission line and the shorted delay line.
4. Part of the step function propagates along the delay line and reaches the short circuit, whereupon the polarity of the pulse is reversed and it is reflected back along the delay line returning after time $2t_d$, where $t_d$ is the line delay time.
5. When the reflected signal appears back at the line input, the diode is reverse biased such that only the load is across the line, and, assuming perfect impedance matching, no further reflections take place.

6. The reflected portion of the step function meets the original, unreflected part with an effective phase difference proportional to the length of the delay line. The two step functions sum such that, except for a short duration pulse once every input drive cycle, the effective output is zero. The waveform is then passed through an ordinary diode to remove noise and spurious transient arising as a result of imperfect matching and phase differences. The result is a clean pulse train of the same frequency as the driving waveform.

An important point to note is that the driving waveform must have a fast enough transition time to effectively reverse bias the SRD before the stored charge is removed, otherwise the abrupt change in voltage will not occur. In other words, the drive frequency of the device has a minimum value below which the reverse bias will not occur before the end of the charge storage phase. In this application, the problem can be avoided by the use of a Schmitt trigger circuit to transform the sinusoidal clock waveform into a square wave featuring a much faster transition edge. Moreover, this limitation also suggests that the generator works more efficiently at higher frequencies.

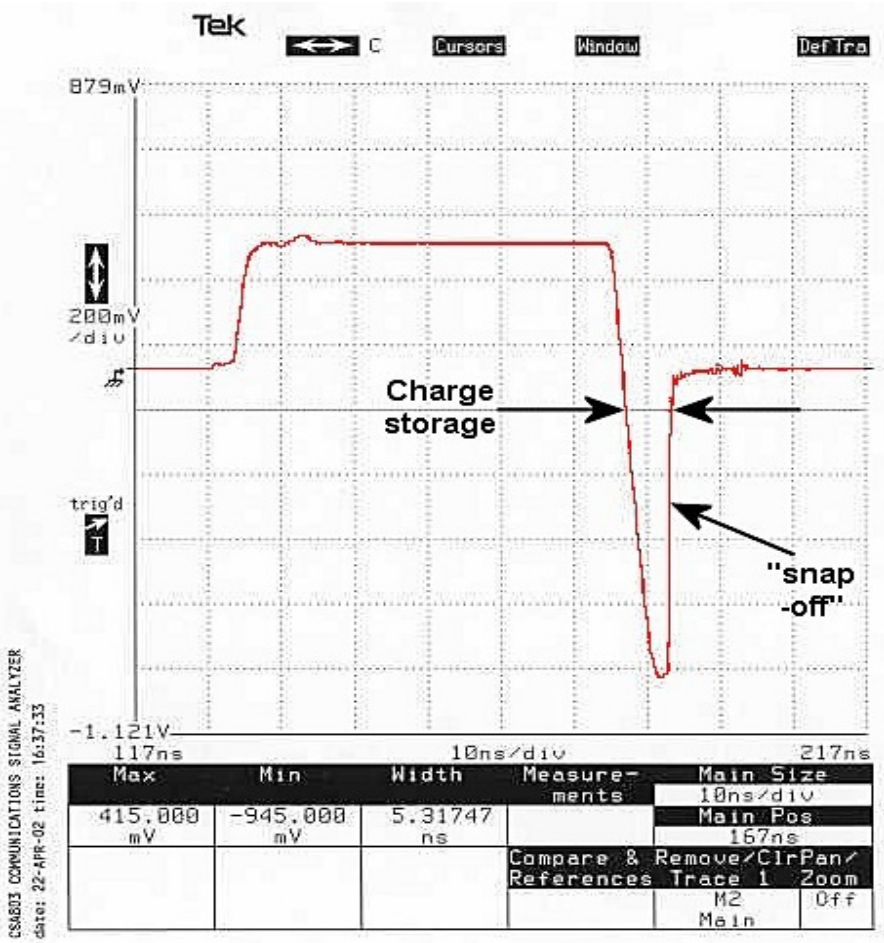


*Figure 6.5. An example of an SRD (Metellics MMD0840) driven by a squarewave. The charge storage and "snap-off" regions can be clearly seen.*

Another feature of this circuit is that the output pulse duration bears no relation to the input waveform. It is governed by the length of the delay line and will have a much shorter rise and fall times than the input pulse, and, depending on the length of the delay line and the reverse recovery time ("snap-off" time) of the diode, pulse widths down to ~100ps can be obtained. The width of the pulse can be approximated by:-

$$t_d = 2\frac{L_d}{V_p} \qquad (6.1)$$

Where $L_d$ is the length of the delay line and $V_p$ is the phase velocity along the delay line. Clearly if the delay line is shorter than the transition time of the SRD the pulse will not evolve to its full amplitude and will be dominated by the SRD transition time rather than the delay line length.

#### *6.8.1.2 Pulse generator construction*

A prototype pulse generator was constructed on a small piece of FR4 Copper clad glass fibre/resin laminate board. The tracks were cut with a scalpel and the components soldered directly to the board in an attempt to minimise parasitic effects. For preliminary experiments, several axial lead packaged Metellics MMD0840 Step Recovery Diodes were procured. The shorted delay line was made from a piece of RG174 coaxial cable with an adjustable short circuit provided by a steel map pin. Input and output connections were provided by means of SMA connectors. A photograph of this simple circuit is shown below:

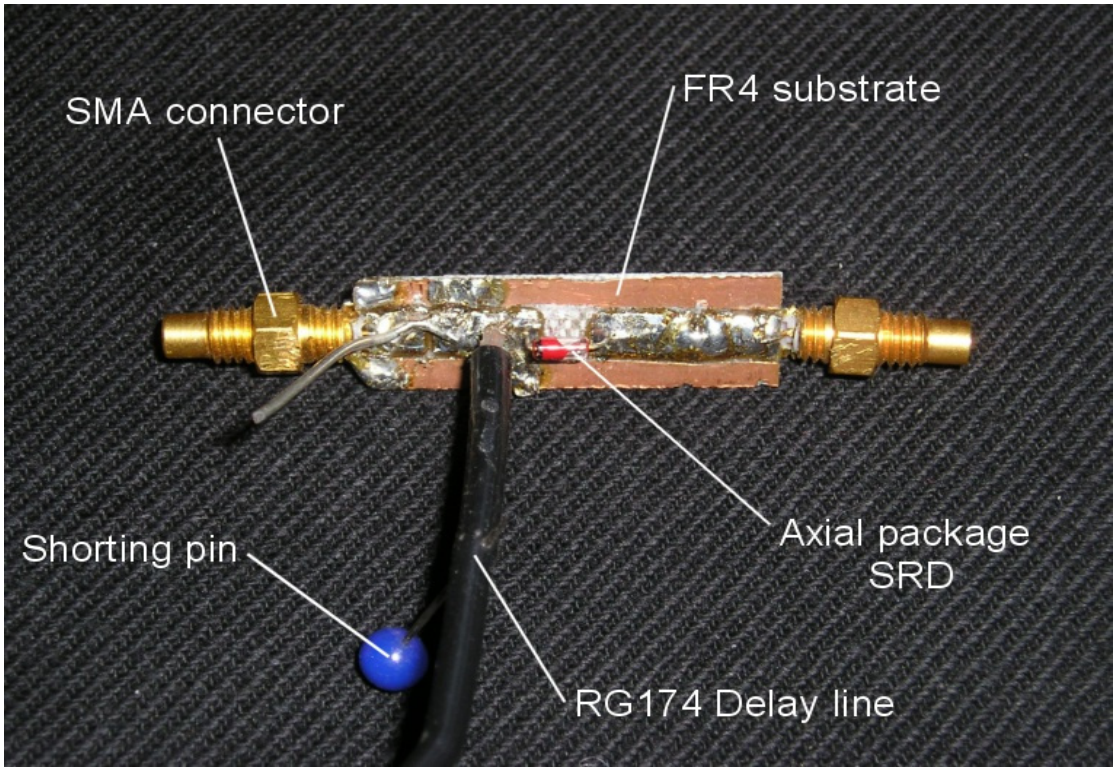


*Figure 6.6. A prototype SRD pulse generator test circuit.*

The prototype circuit was then connected to a suitable pulse generator and a 4v peak to peak square wave signal was applied. The output of the device was connected to a Tektronix CSA803 communications signal analyser. The resulting output pulse can be seen in the figure below: The prototype generator output exhibits excellent quality symmetrical pulses of approximately 300ps duration. A low level of ringing also shows good impedance matching characteristics (and consequently, a low chance of laser afterpulsing and efficient power transfer to the load).

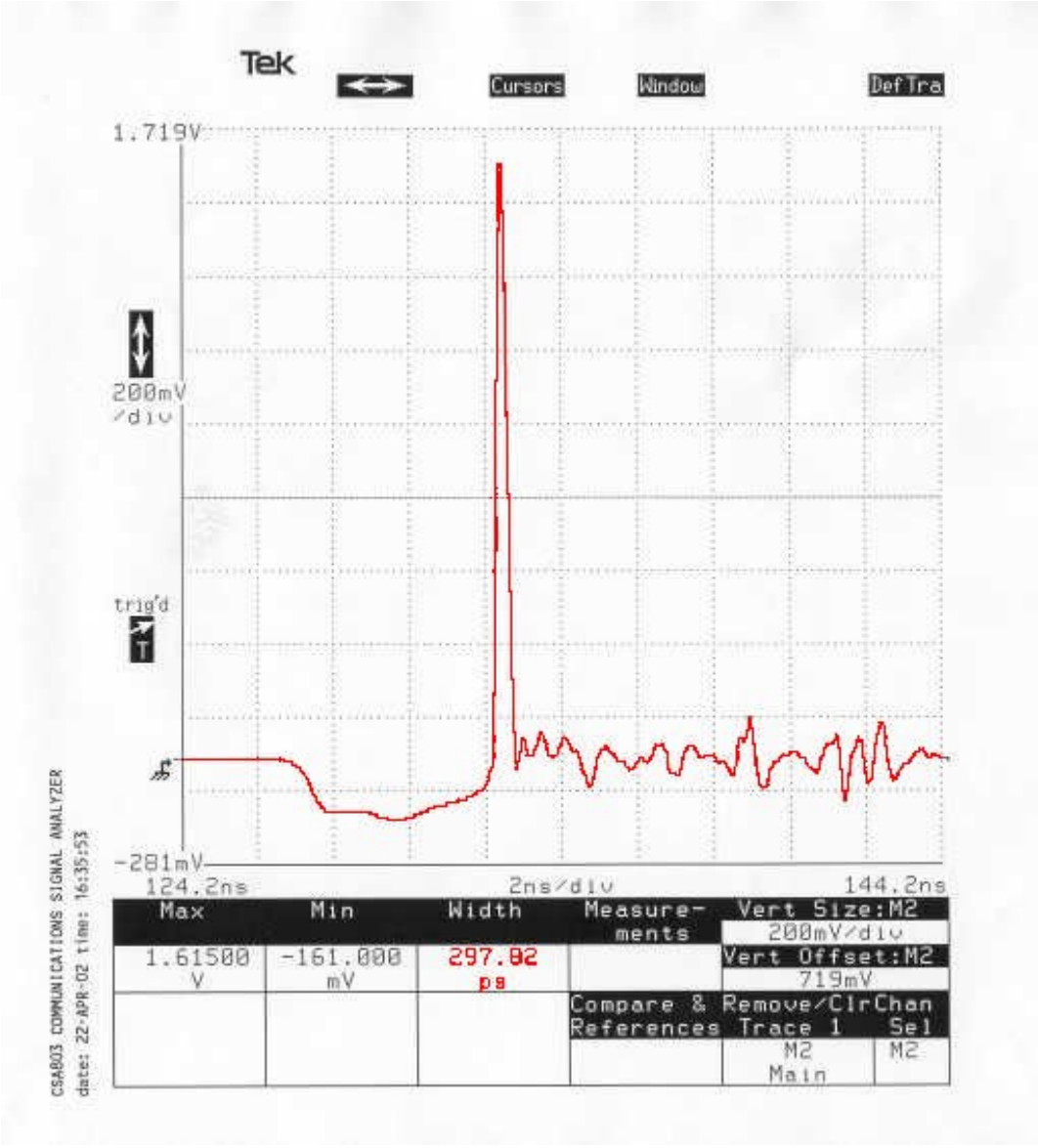


*Figure 6.7. An output pulse from the prototype pulse generator showing a clean pulse of approximately 300ps width.*

The resulting pulses were excellent given the crude method of construction and the low component count and were deemed suitable for use as drive pulses for laser diodes. The output pulse height was dependent, to some extent, on the voltage of the drive signal, showing promise for future implementation of control over the pulse amplitude.

### *6.8.2 Alice driver PCB development*

The object of this work was to design a compact, professional quality printed circuit board for use inside Alice modules. The design was to contain all of the necessary circuitry to drive a free-space QKD transmitter (including the new pulse circuit).

Over the course of the three years of development of this system, three design iterations were made, each building on the successes of the previous circuit:-

- Prototype stage: Designed with four channels for testing the basic circuitry.
- Alice driver mark I: Designed to implement the above circuit with improved circuitry and professional software-based PCB design and manufacture. Several additional features included.
- The third design stage was implemented later in the programme and is described in a subsequent chapter.

#### *6.8.2.1 The prototype Alice drive circuit*

This circuit was designed as a proof of principle to show how the fast pulse generator and its associated circuitry would operate in a real system. The circuit was designed to pulse four laser diodes at a frequency of 10MHz provided by the GT300 frequency standards used previously. An overview of the circuit is shown below with a description of operation:

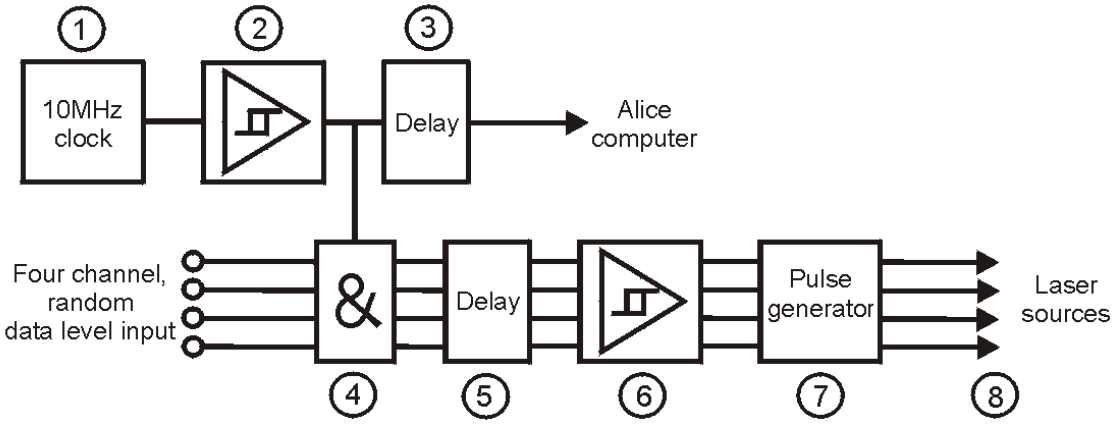


*Figure 6.8. Diagram showing the prototype circuit designed to pulse four laser diodes at 10MHz.*

1. A stable oven controlled crystal oscillator provides a 2V peak to peak sinusoid at a frequency of 10MHz.
2. The sinusoidal clock signal is squared using a low output impedance broadband op-amp in Schmitt trigger mode. The squared output is then split with one part being fed to an integrated circuit active delay whilst the other part is fed to a quad NAND gate (7400 FAST technology).

3. The delay allows the computer DIO card to be synchronised to the rest of the system such that the voltage levels from the DIO card arrive at the NAND gate synchronously with the clock pulse. This facility also allows connecting cables of varying length to be used.
4. The clock signal arriving at the NAND gate is combined with the voltage levels supplied randomly by the DIO card data output channels. This arrangement acts as a clock recovery circuit for the data channels, restoring each signal to zero at the end of a clock pulse.
5. The four TTL data channels are then each passed through a manually set active delay line to allow inter-channel jitter de-skewing.
6. The four signal channels are each applied to a wideband amplifier with a high output current capability acting as a driver for the delay line pulse generator.
7. The device chosen for the driver was a Texas Instruments OPA699 voltage limiting amplifier. This amplifier has the facility that one can limit the output voltage excursion to a preset level by applying a control voltage to a pair of dedicated pins. This facility allows some adjustment in the amount of current delivered to the pulse generator, and thus the amount of energy delivered as a pulse to the laser diode. In short, this can act as an intensity control for the laser diodes.
8. The amplifier was connected as an adjustable Schmitt trigger allowing the device to be triggered anywhere on the edge of the incoming signal pulses, thus providing a trim function for the pulse timing. This arrangement also converted the TTL compatible signals to the bipolar waveform required for the pulse generators. The outputs of the four amplifiers fed a set of four SRD pulse generator circuits of the type described above in section 6.8.1. Short random pulses were delivered to the laser diodes resulting in randomly polarised pulses of light at the output at a rate of 10MHz.

Although the pulse repetition rate of the system was designed to be 10MHz, the generation of pulses of the order of 1ns width implies the presence of frequency components up to several gigahertz (GHz). Consequently there was a requirement to use high frequency construction techniques such as earth planes and robust power supply decoupling during circuit fabrication.

The circuit was constructed on FR4 copper clad board and connected to a prototype Alice optical system (shown below) the combination was used in several key exchanges.

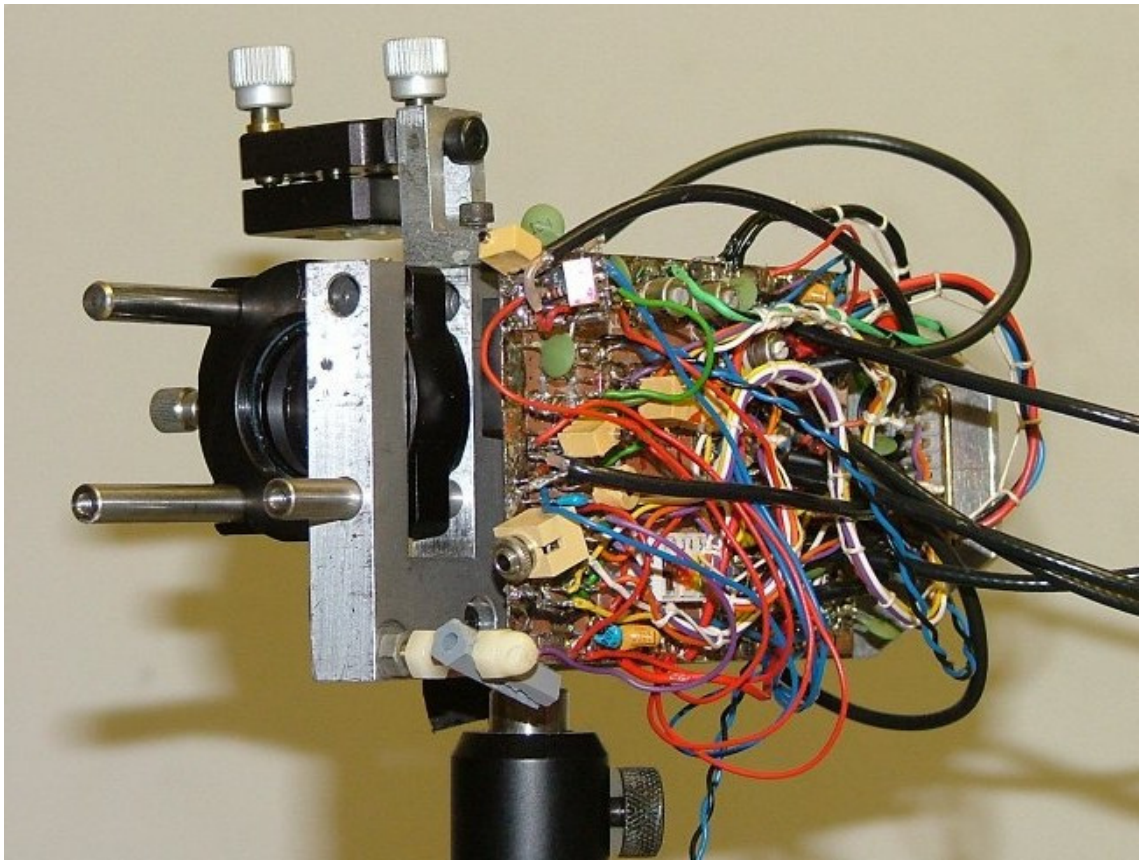

*Figure 6.9. A photograph of the prototype Alice complete with drive electronics, four laser sources and coupling optics. The device would be mated to a suitable telescope when used. This system was an order of magnitude smaller than the demonstration system described previously being approximately 100×140×80mm.*

#### *6.8.2.2 The Alice "mark I" PCB requirement*

With the successful demonstration of the proof of principle circuit, design work for a complete drive circuit for a practical QKD transmitter to be committed to a PCB commenced. The target specification is shown below:

- Provision of four pulsed data channels, each capable of running from 500kHz to 10MHz, with an optical output pulse width of 1ns and a delay resolution ≤500ps (this means that the four channels must all emit pulses within 500ps of each other under diverse operating conditions).
- Onboard generation of an extremely stable and accurate clock signal running at 10MHz with a stability of $\leq \pm 3 \times 10^{-10}$ per day or $\leq \pm 5 \times 10^{-8}$ per year (i.e. better than the GT300 frequency standard).
- Provision of a "recovered clock" signal with variable delay for transmission to the controlling computer for synchronisation purposes.
- Provision of four continuous wave data channels to allow continuous bright emission for alignment purposes.

- Provision of a switched output for a bright alignment source.
- Provision of on-board stabilised power supplies for the circuit and add-on items such as an optical beacon and tracking camera.
- Provision of the above on a small circuit board (~120mm×80mm), with a current requirement of ~1 ampere.

The first two requirements have already been discussed above and placing the circuitry on a purpose-built PCB would normally lead to a modest increase in performance due to reduced parasitic inductance and capacitance arising from the improved circuit construction.

The final five requirements were specified as a result of experience gained during the previous trials work and are described below. The design philosophy for this circuit was to keep the system cheap and simple using off-the-shelf components where possible.

#### *6.8.2.3 Stable clock design*

The breadboard and prototype QKD systems utilised oven stabilised 10MHz frequency standards to provide synchronisation between the two data terminals. Although accurate enough, these oscillators were bulky and required their own additional power supply. It was decided to include the clock generation circuit in the Alice electronics interface and eliminate the extra cabling and power supplies associated with clock distribution.

The device chosen for the system clock was a C-MAC CFPO-4 high stability oven controlled crystal oscillator (OXCO). This device outputs a 10MHz sine wave at 2Vpeak to peak amplitude into 50Ω [16]. The OXCO stability is specified as: $\leq \pm 7 \times 10^{-11}$ per year or $\leq \pm 1.2 \times 10^{-8}$ per day which was considered excellent given the size of the package (40×30×20mm).

A test was conducted to assess the comparative accuracy of a pair of clocks over a wide temperature range of the sort that might be encountered during operation of a QKD system in various environments. The test involved sampling the output of both clocks and comparing their relative frequency. Results of this test are shown in Figure 6.10 below. The graph shows the difference in frequency between the two OXCOs procured for this design. It can be seen that a 33°C relative environmental temperature change produces an almost immediate reaction in the relative clock frequencies. Only a 5mHz change in frequency between the two clocks occurs over this range.

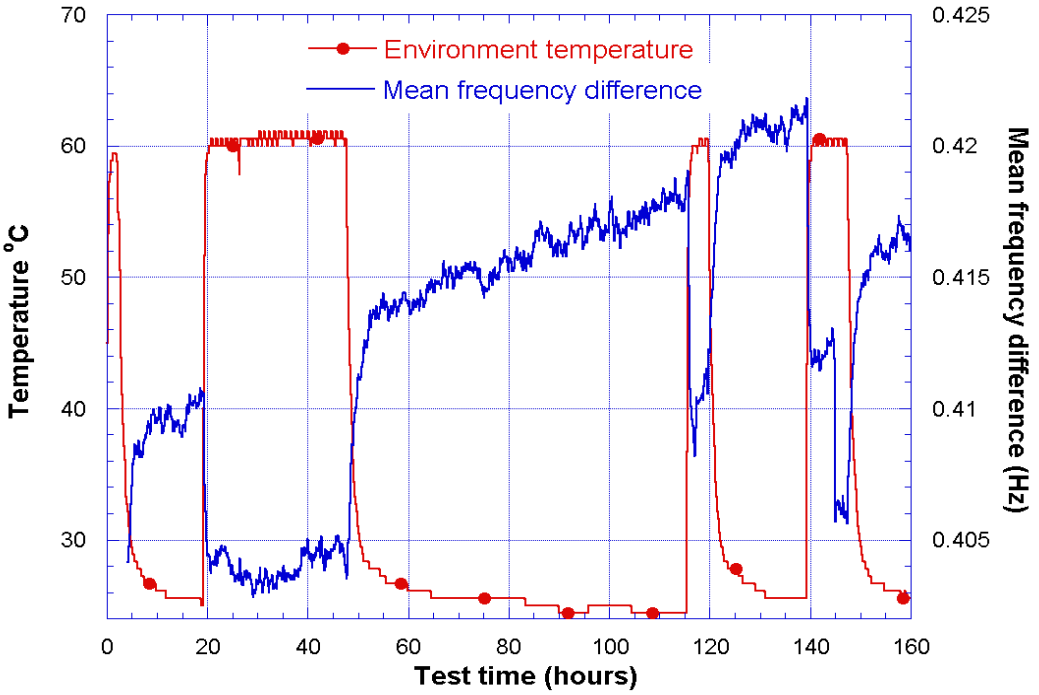


*Figure 6.10. Relative change in clock frequency between the two compact clocks subjected to 33$^{o}$ Celsius temperature change.*

The overall upward drift of the clock frequency is probably due to initial ageing of the clocks and can be neglected for our purposes since it occurs over a long period. Furthermore, the OXCOs posses a trim function for tuning out small errors. The indication is that these miniature devices are suitable for synchronising the QKD terminals.

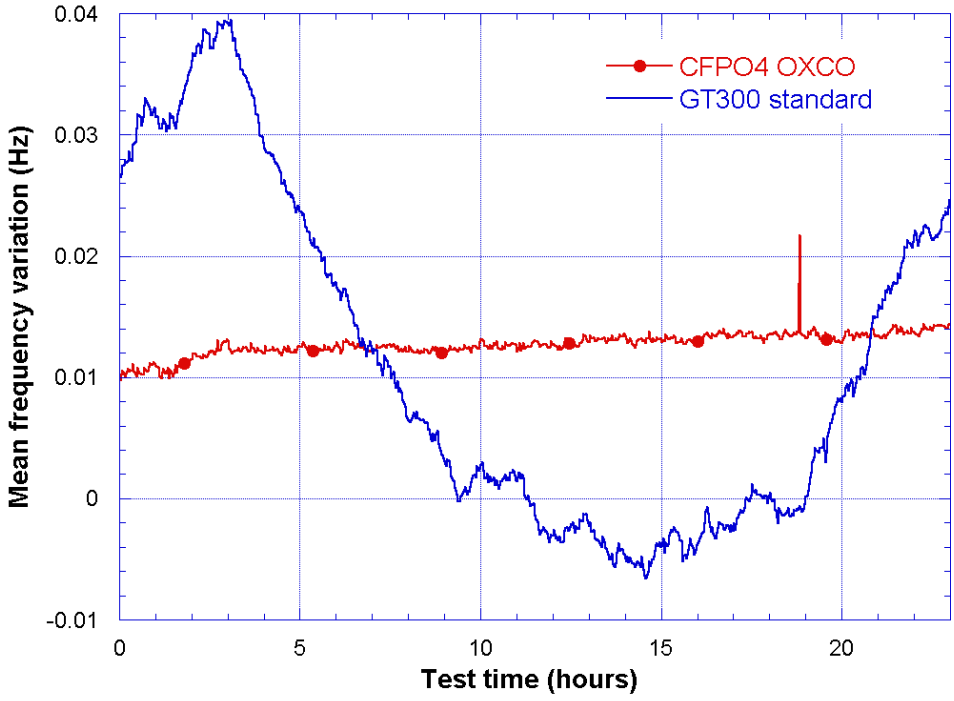


*Figure 6.11. Comparison of compact clock and original frequency standard.*

By way of comparison, the graph above shows the frequency variation between the new and the old clocks, over 23 hours, with reference to one of the new clocks.

It is clear that the original frequency standard makes significant deviations over a matter of a few hours (notwithstanding, this clock is still extremely accurate and still suitable for QKD systems). However, examination of the trace for the new OXCO clock shows a smooth, stable trace with a frequency variation of less than 10mHz. This shows that the two new clocks are extremely well matched and ideal for use in the system.

#### *6.8.2.4 Alignment aids*

The remaining additions to the design count as alignment aids. As stated elsewhere in this thesis (chapter 5, section 4), optical alignment of the two terminals of a QKD system can be exceptionally arduous and time consuming. With this in mind a layered approach to alignment was adopted. Firstly, a bright flashing LED beacon was proposed as a general sighting cue.

Secondly, a bright alignment laser was added to the optical system and arranged such that its divergence was greater than that of the four data channels, thus providing a much wider, brighter cone of light to capture. Typical values of divergence used were 250µrad for the data beam and 1mrad for the alignment beam. Finally, the four data sources were provided with the ability to emit continuously. Thus, once the coarse alignment had been achieved, the bright alignment source was switched off and the data channels switched to CW mode allowing fine alignment. Once aligned the sources were switched back to QKD data mode. All alignment aids were provided with electronic switches such that they could be operated from the controlling computer.

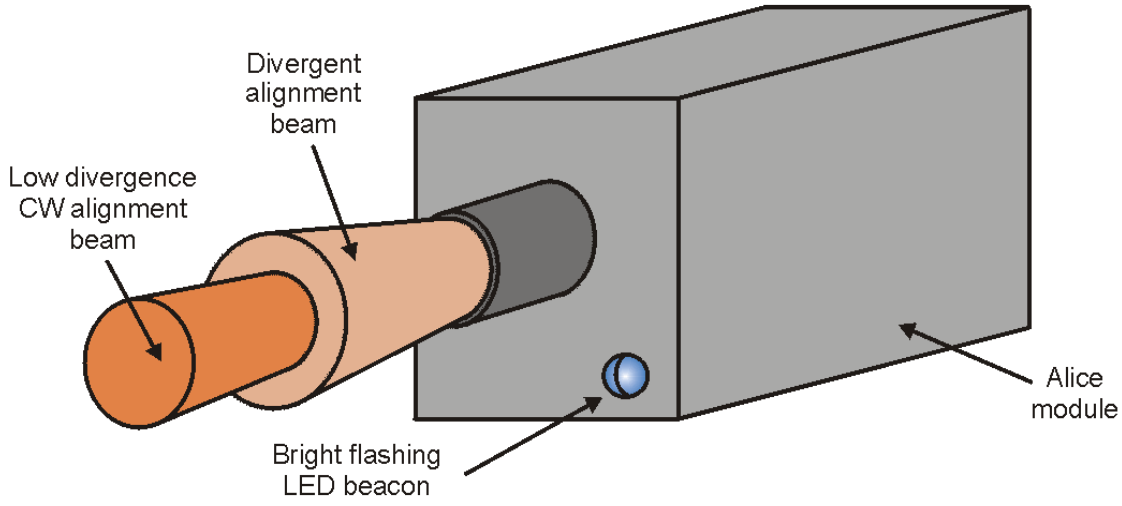


*Figure 6.12. Alignment methods for Alice. A flashing beacon provides a visual cue for location whilst switchable beams of varying divergence provide an alignment aid.*

### *6.8.2.5 Power supplies, circuit board and miscellaneous*

The new PCB was supplied with +5V and +12V, via umbilical cable, from the power supply of the controlling PC. The 12V was fed directly to the OXCO whilst the 5V supply was conditioned by a DC-DC converter delivering +/-5V to the PCB with a current capability of +/-500mA.

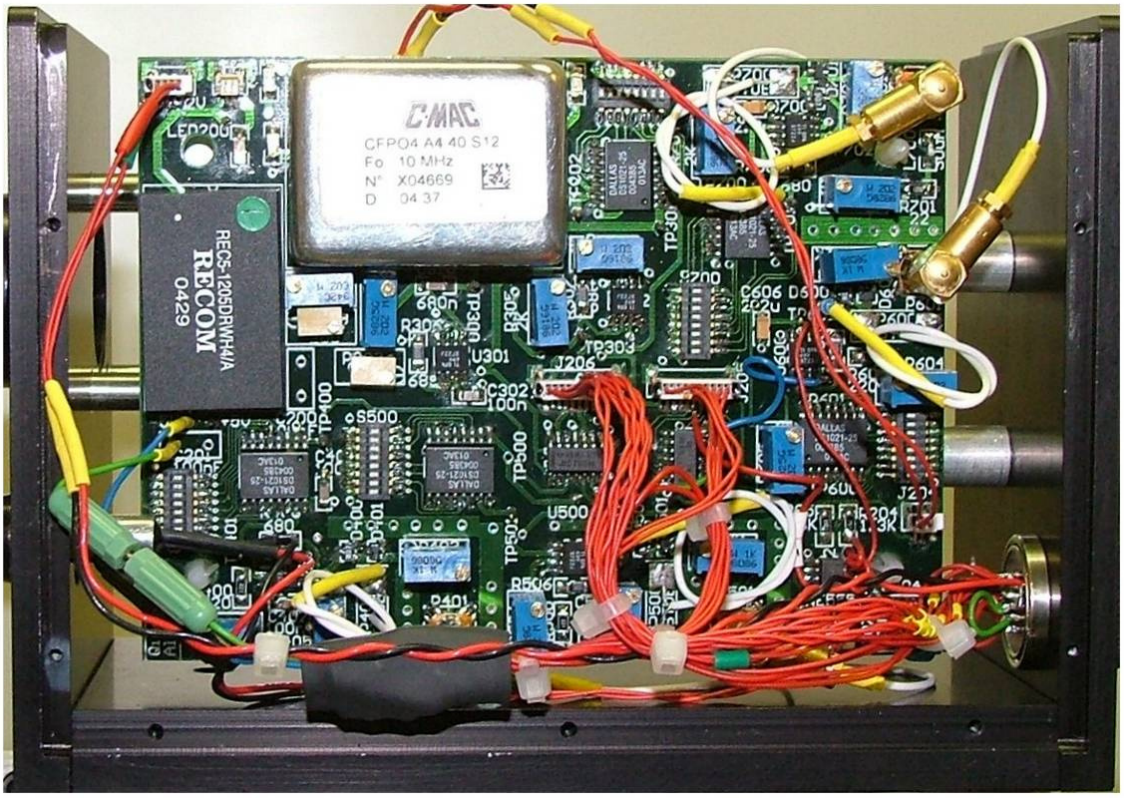


*Figure 6.13. Image of the completed Mk I Alice PCB. Note the 18 adjustment pots. Five miniature DIP switches for setting the delay on each channel are also visible. Delay lines for the pulse generators may be seen as coiled white co-axial cables The board mounts securely to the rear side of the optical bench.*

The umbilical cable was made from good quality shielded signal cable (Brand Rex BE57509, 9 pair, shielded cable). Multiple conductors were commoned for power transmission while each signal was carried via single twisted pair. Connections at both Alice and the computer were made via a high quality 24 way circular connectors (Binder 723 series).

PCB fabrication was outsourced to a commercial manufacturer (Beta-Layout Ltd) and resulted in a professional quality, cost effective solution. The board was manufactured in a 4-layer process using standard FR4 substrate. The finished, populated board may be seen in Figure 6.13 above.

### *6.8.2.6 Alice optical bench and system housing*

With the new electronic design came the requirement for a compact optical system with the capability of coupling four pulsed laser diodes into a single mode beam. The configuration chosen was similar to the generic optical layout discussed in chapter 4 of this thesis. The new optical system was specifically designed to minimise the effort and complexity of aligning the Alice optical system.

The high divergence of the laser sources was exploited by moving the sources closer to the beamsplitters and pinholes and allowing the beam to diverge freely. In this way the need for laser collimation and angular adjustment was removed. All optical components were mounted on an optical chassis approximately 120×90mm. The four laser diodes were grouped into two pairs with each pair being mounted in a carriage which allows individual vertical adjustment of each laser. The light from each laser in a pair was then coupled together using a beamsplitter. The beams from each pair were then coupled together using a third beamsplitter with the output beam from all 4 lasers directed towards a 100µm pinhole. Horizontal adjustments were made by rotating the beamsplitters to overlap the emission from each laser.

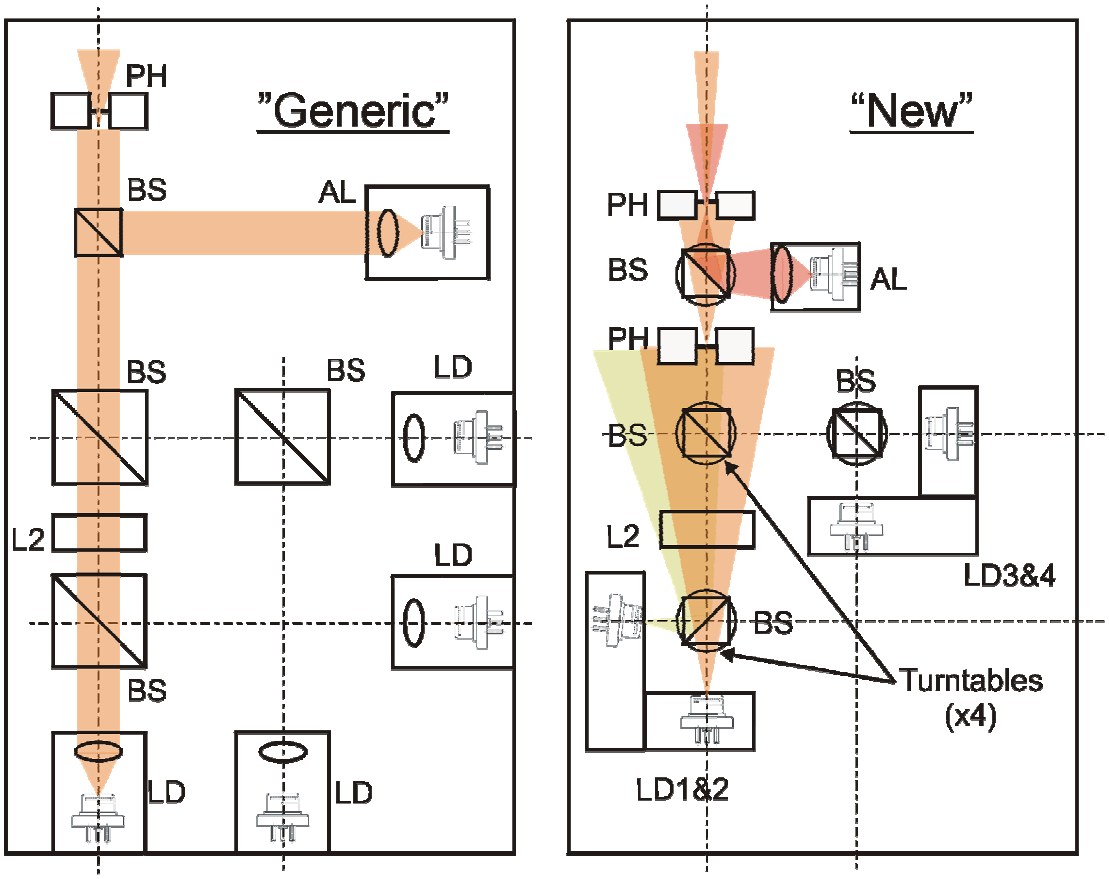


*Figure 6.14. Comparison of the Generic and New optical layouts showing how the "new" system saves on adjustment and allows coupling of an alignment source. The effects of source misalignment can also be seen for LD2 (light green).*

By way of comparison, with reference to Figure 6.14 above, one can sum the degrees of freedom (DoF) of adjustment required for aligning the “generic” and “new” optical systems. With the old system, 35 individual optical adjustments were required. The new chassis reduced this to 17.

Ultimately the direction of the light transmitted from Alice is determined by passing the light through a second 100μm pinhole separated from the first by 25mm. This ensures that the light from all 4 lasers is axially aligned and that an eavesdropper cannot infer which laser is firing by observing subtle differences in the direction of travel of the photons. A novel feature of this system was the incorporation of an additional laser source to aid with alignment of Alice and Bob over large distances. The 650nm wavelength laser was positioned between the 2 pinholes and co-aligned with the 4 single photon sources using a further beamsplitter. The beam was arranged to have a higher divergence than the data lasers but was also much brighter making it easy for a tracking camera to acquire. This facility also offers the possibility of using the alignment laser as a continuous tracking beacon as well as a communications source for a classical channel. The new optical bench was manufactured using CNC machining techniques with standardised components such as beamsplitter turntables and laser diode holders. A CAD drawing of the optical system can be seen in Figure 6.15:

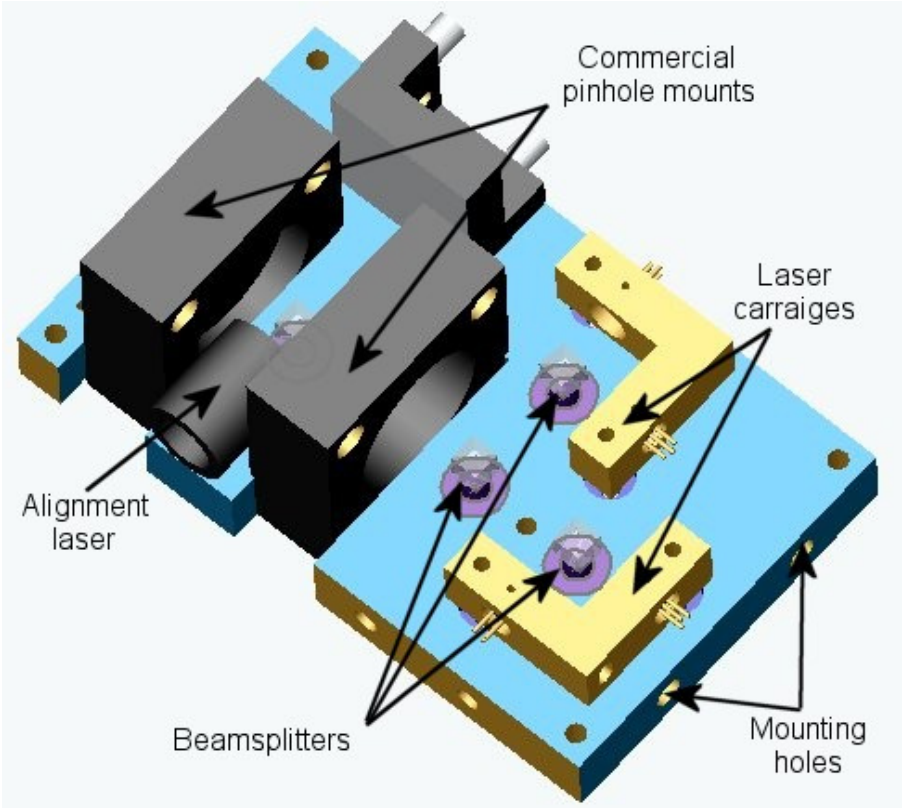


*Figure 6.15. 3-D CAD drawing of the final Alice optics design (Design drawing courtesy of Dr. D. M. Benton, QinetiQ, Malvern).*

In the final system, use was also made of commercial optical mounts for the pinholes.

As mentioned above, connectors, termination and cabling is often neglected in so-called “Beta” systems. In this case, with a production run of three systems, wiring and termination was standardised with good quality connectors and cabling specified in an effort to bring the system closer to a more productionised form. The complete system, including drive electronics and stabilised clock was mounted in a black anodised aluminium frame with a close-fitting sheet Aluminium cover also anodised black and measured approximately 200×150×100mm. A photograph of Alice showing the optical system is shown below in Figure 6.16.

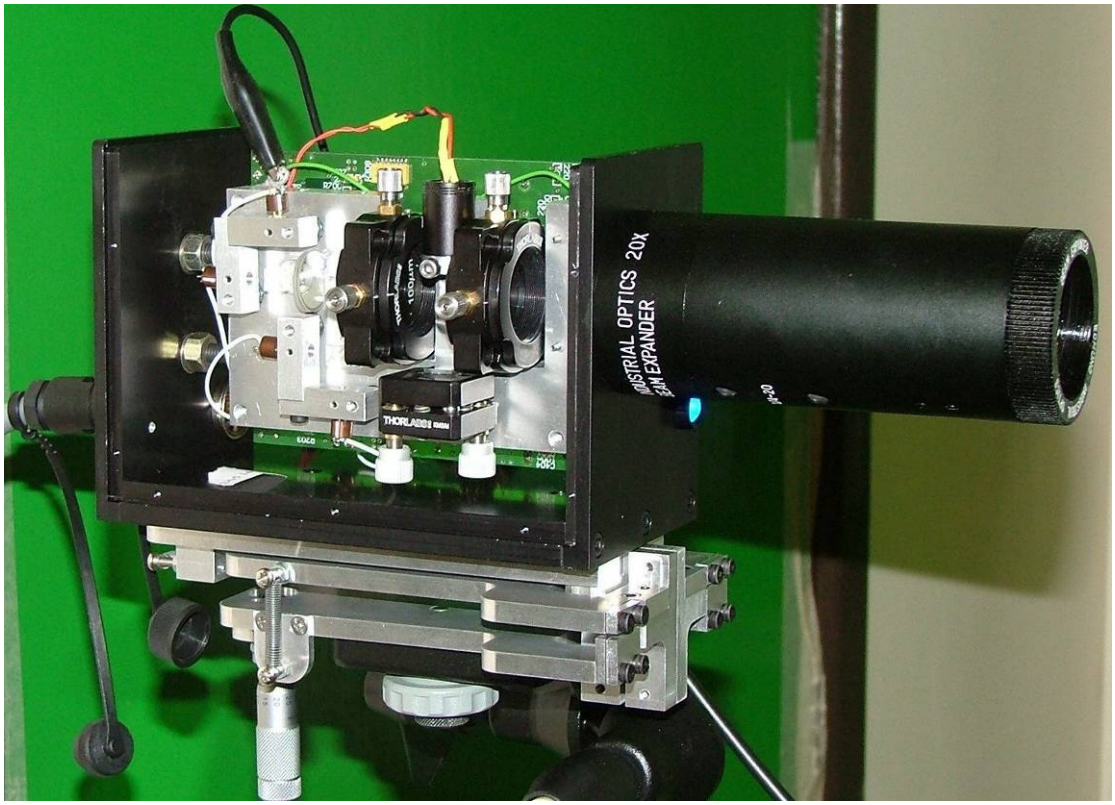


*Figure 6.16. Photograph showing detail of the Alice module mounted on the fine adjustment stage. The optical system is clearly in view whilst on the front panel one can see the bright LED beacon.*

### *6.8.3 The compact Bob receiver*

The design of a new Bob receiver module, complete with optics and programmable electronics was proposed as part of the development of the QinetiQ system. Whilst the design progressed, difficulties with the development of the novel shallow junction photon counting detectors led to long delays and the decision was made to use the LMU Munich designed Bob receiver which had proven to be an extremely reliable and useful device.

#### *6.8.3.1 Munich Bob*

Work package 1 of EQCSPOT dealt with the design and fabrication of miniature modules for QKD. One of these pieces of hardware was a receiver module. This was a device which co-located all of the optics, detectors and electronics required for a QKD receiver into one small package. The group responsible for this work (including Christian Kurtsiefer, Mattheus Hälder and Patrick Zarda, working under Professor Harald Weinfurter) at Ludwig-Maximillians Universität, Munich, produced some extremely innovative hardware which, although originally designed for use with fibre optic systems, was, with some redesign, suitable for free-space systems.

#### *6.8.3.2 Receiver optical design*

The operation of the receiver is typical in that light is gathered and focussed by an external telescope (common mountings on the Bob enclosure such as a "C" mount ensured compatibility with a wide range of telescope fittings).

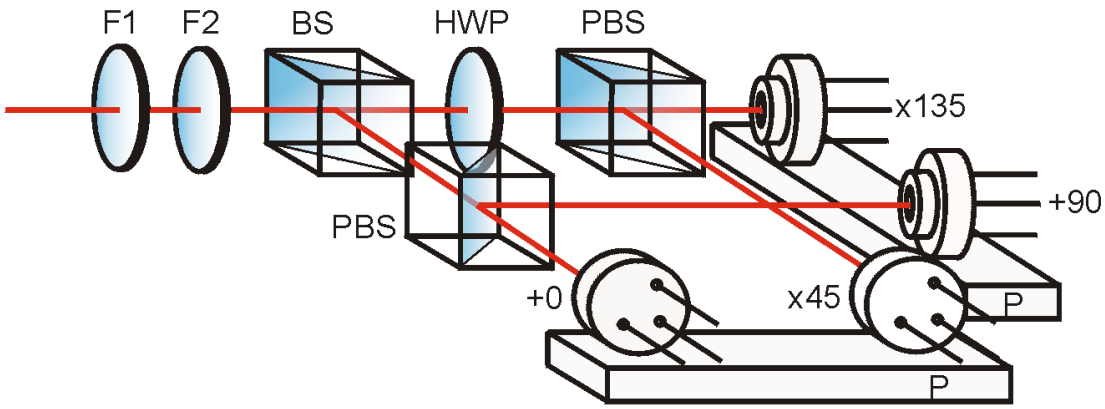


*Figure 6.17. Optical layout of the "Munich" Bob module. Practical innovations include four detectors mounted on a pair of cooling blocks with individual Peltier (thermo-electric) coolers.*

The light is strongly filtered to reject any background and then randomly switched at the beamsplitter (BS).

Half the photons are passed through a polarising beamsplitter (PBS) and analysed in the +0/+90 detectors (i.e. the rectilinear basis) whilst the other half of the incoming light is first passed through a half-wave plate (HWP) to rotate the polarisation state through $45^{o}$. The rotated light is then analysed in the ×45/×135 detectors (i.e. the diagonal basis). Detectors are housed in cooling blocks which are thermally bonded to Peltier coolers (P). The optical layout of the LMU Bob module is shown above in Figure 6.17.

#### *6.8.3.3 Electronics*

The single photon detectors were a set of four, matched, Perkin-Elmer C30902 Silicon avalanche photodiodes operating in passively quenched Geiger mode. Each of the four detectors is biased by an adjustable high voltage DC-DC converter at a bias voltage of around 15V over the avalanche voltage. The SPAD output pulses are discriminated by an ECL line receiver with a preset variable trigger level and then fed through a "D"-type flip-flop to a high frequency output amplifier. This results in a NIM (nuclear instrumentation module) compatible output pulse whenever a photon is detected.

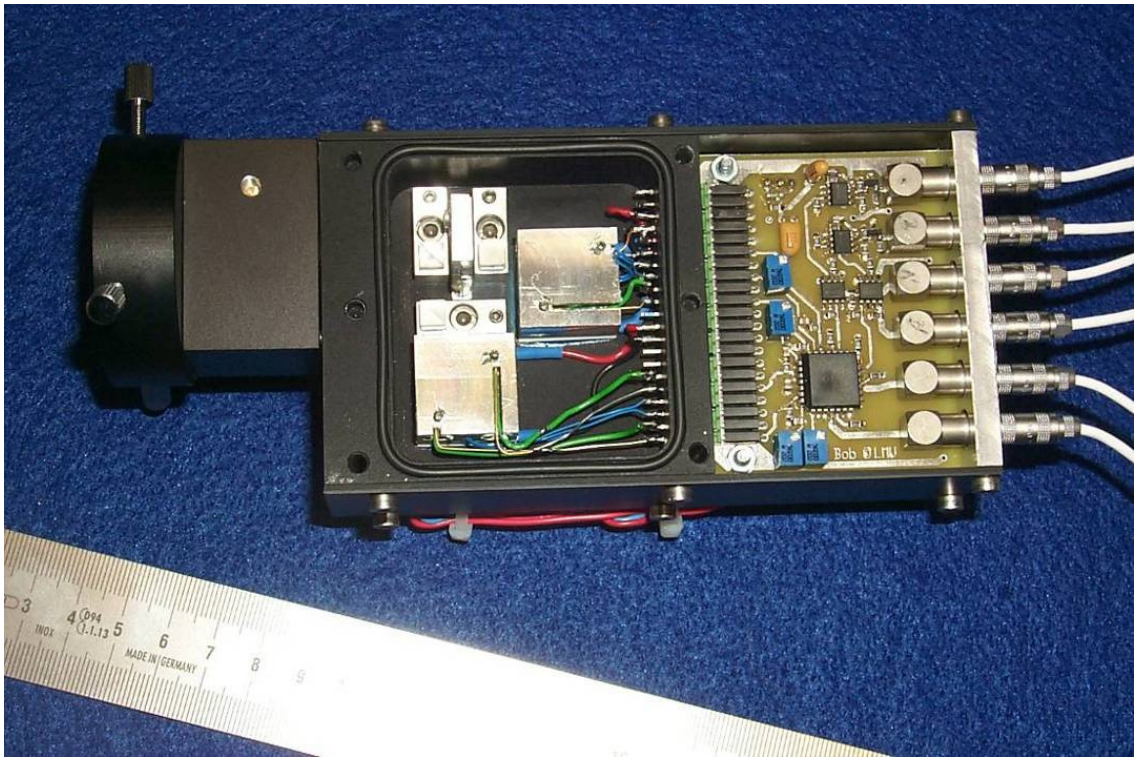


*Figure 6.18. The "Munich" Bob module showing optics, detectors and electronics compartment.*

The complete electronics package is housed in a separate compartment, attached to the Bob module. The module is shown in Figure 6.18 above.

#### *6.8.3.4 Innovations*

The SPADs are mounted in two cooling blocks, each mounted on a Peltier cooler with the “hot side” thermally bonded to a heatsink. The heatsink is cooled using an electric fan. The module includes a wired electrical delay line (Note the bottom four outputs) and an ECL OR gate. This function allows the four detectors to be multiplexed onto two output channels (a similar function to the optical delay line in the breadboard Bob described in chapter 5). This avoids the problem of bandwidth limitation due to detector dead time (by a factor of two). Furthermore, whilst the receiver possesses four detectors, this method also allows the use of a single time-stamping card in the associated computer system, thus costs can be minimised (a two-channel GT 653 time interval analyser card can cost >$5000).

#### *6.8.3.5 Drawbacks*

After long and repeated use, it is not unknown for the cooling blocks or the Peltier coolers to become separated from the heatsink. This causes the detectors to cease functioning in the correct mode. If this happens, problems can also arise with detector alignment. A complete optical overhaul is required in this unlikely event. A case of incorrect alignment resulting from this situation can be seen below in Figure 6.19.

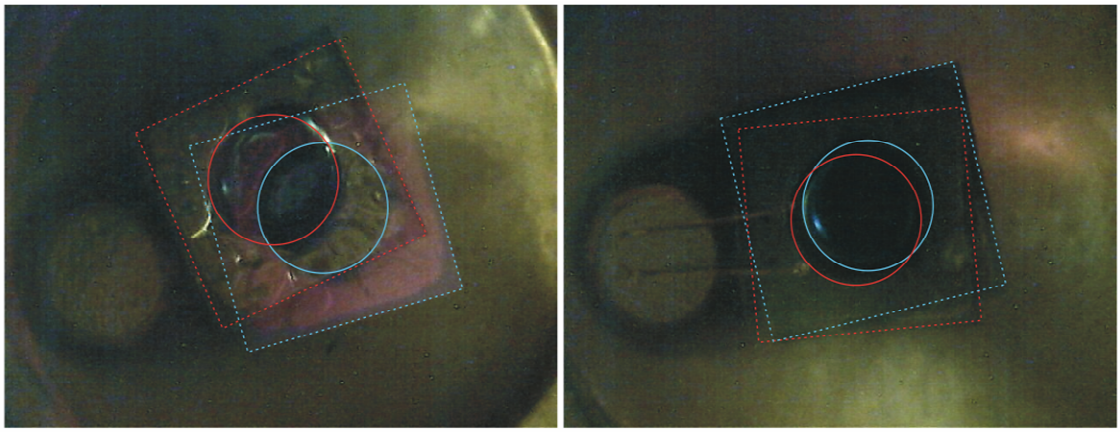

*Figure 6.19. Munich Bob detectors as viewed from the module output aperture. Detectors 1&2 (left) appear to suffer from a gross misalignment. Conversely, detectors 3& 4 are fairly well aligned.*

Ideally detectors would overlay each other and both pairs would also overlay each other. Figure 6.20 shows the same detectors but with all four devices superimposed. Dotted squares denote the outline of the detector chips whilst the solid circle denotes the active area of the detectors.

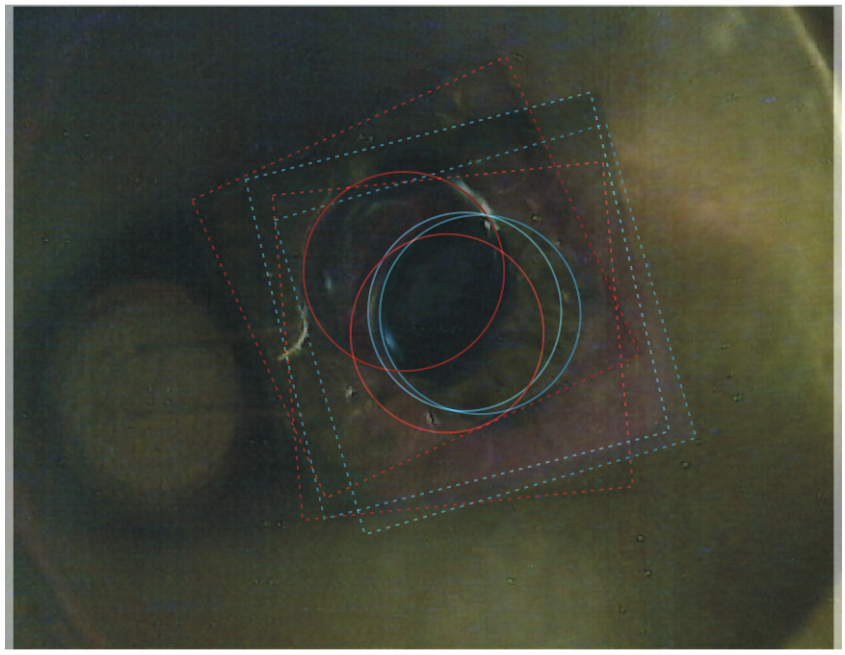

*Figure 6.20. All four Munich Bob detectors as viewed from the module output aperture. Clearly this module requires re-alignment.*

The Munich Bob used by QinetiQ also experienced a reduction in detector efficiency over some years but this is probably due to detector aging and the extreme uses to which the module has been subjected rather than the design of the device itself.

#### *6.8.3.6 Conclusion*

The Munich Bob is an excellent piece of engineering and comes in a highly usable form. The module is robust, compact, lightweight and extremely reliable. The Munich Bob used by QinetiQ in QKD experiments has seen service over several years in extensive trials and QKD systems with only slight modifications from the original design.

### *6.8.4 QKD Software and algorithms*[10]

The operating software for the compact system was much the same as that used in the breadboard system (described in detail in chapter 5, section 5.3.3), which operated with a software suite capable of performing real-time key exchange, sifting, error correction from its initial design in 1998. However, in the light of experience of several trials and tests, new functions were added and new diagnostic programmes written to aid set-up and operation of the system. Several modifications are worth mentioning here:

[10] The vast majority of software for the QinetiQ system was written by Paul Tapster. However, it must equally be said that many of the ideas encoded in the software are a result of teamwork over a period of several years and many trials and tests.

***Demonstrator software***

A "front end" was designed whereby the key exchange could be configured and initiated from a simple graphical user interface (GUI). This GUI was also equipped with the facility for demonstrating the use of the keys by capturing the Alice user's image via webcam, encrypting the image with a QKD-seeded DES algorithm, transmitting the encrypted image to Bob, decrypting and displaying the image.

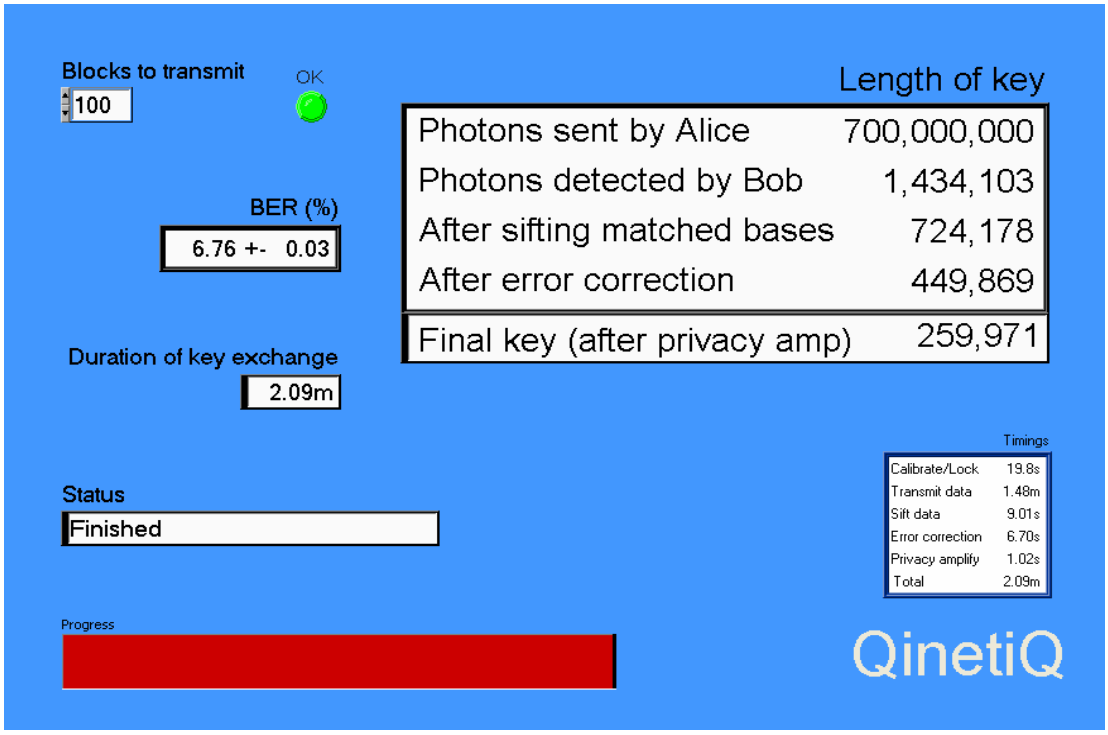


*Figure 6.21. A screenshot of the system GUI showing status, progress bar and important exchange parameters.*

***Mounting hardware***

The system required some means of secure mounting. For the compact version, two ordinary photographic tripods were procured and a pair of identical fine pointing stages were designed and manufactured. The main reason for the bespoke manufacture of the stages was the requirement for an extremely low level of crosstalk between adjustment degrees of freedom. In addition, a simple peg and hole mounting system was devised to allow quick and repeatable mounting and demounting of the system components.

***Output telescope***

This requirement is discussed in depth in chapter 4. Since this version of the system was designed for relatively short ranges, small telescopes were specified for use. For Alice, the telescope chosen was a ×20 Galilean beam expander, procured from Edmund Optics, with an output aperture of 30mm. For Bob, the situation was a little more complex in that the Munich Bob is fitted with a "c-mount" and requires some extra

optics such as a spatial and spectral filter to be included in the optical system. Therefore a simple bespoke telescope of similar optical power to that used at Alice was constructed from laboratory optical components and fitted to the Bob module.

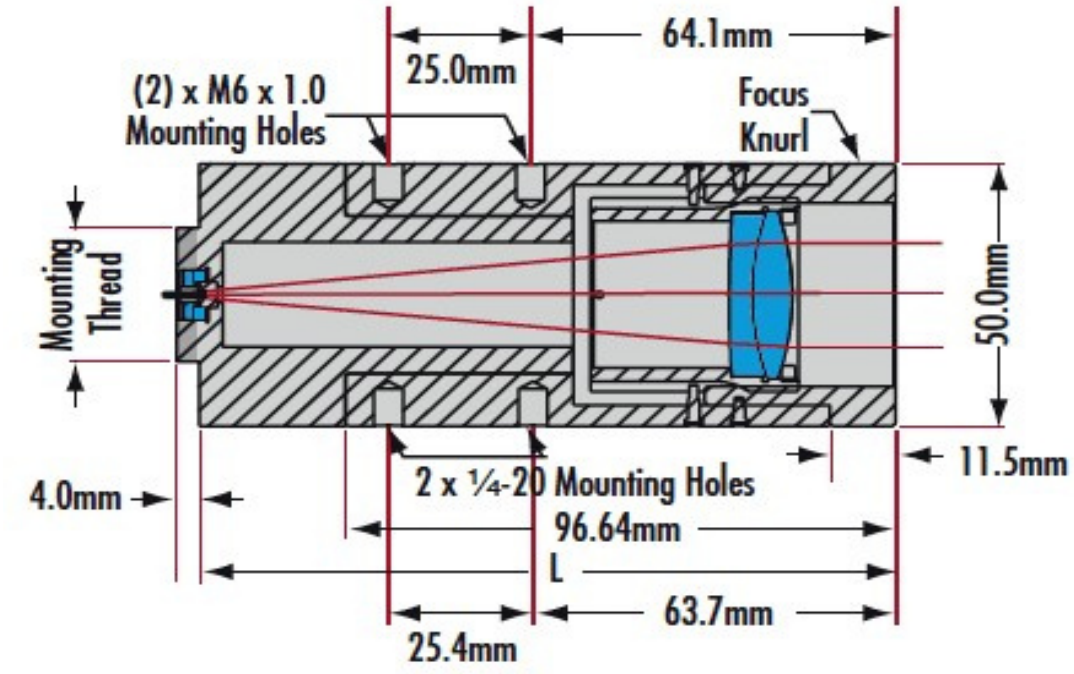


*Figure 6.22. Diagram of the commercial beam expander used for the coupling telescopes in the compact QKD system (image: Edmund scientific corporation).*

***Diagnostics***

A program was written giving direct control over the optical output of the transmitter head. Used in conjunction with "RateCounter.exe", the program called "AliceAlignment.exe" proved invaluable for obtaining optical alignment of the system. The optical output can be switched using the front panel buttons and allows complete control of all optical sources in the transmitter.

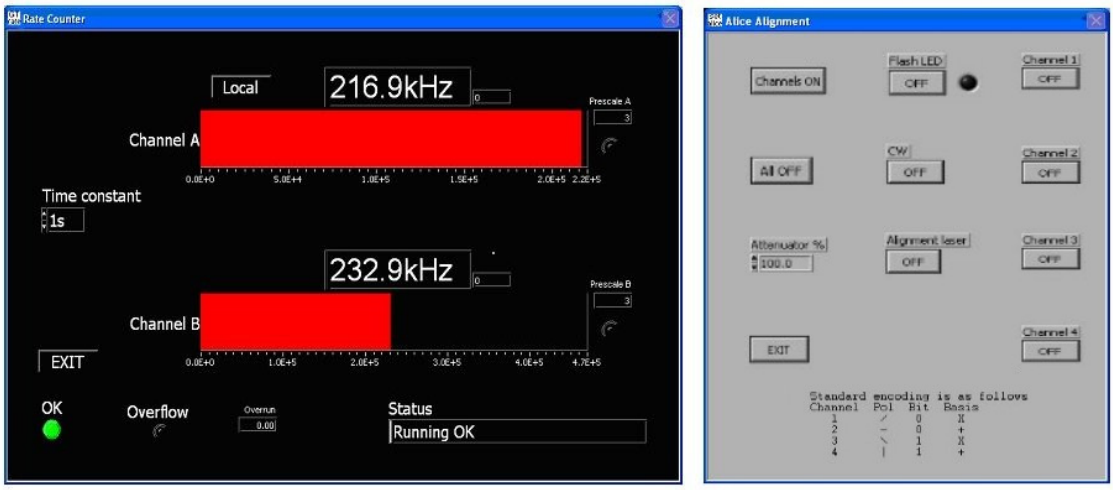


*Figure 6.23. Screenshots of the front panels of RateCounter (left) and AliceAlignment (right) programs used for optical alignment of the system.*

## 6.9 Tests, trials and demonstrations

### *6.9.1 Pulse performance*

The pulse performance is critical to the secure operation of the system. Pulses are required to be uniform in amplitude and width with low channel timing skew, that is, each pulse must be produced at exactly the expected time because any discrepancies in pulse emission could potentially be exploited by an eavesdropper. The pulse output of the Alice Mark 1 PCB is shown below:

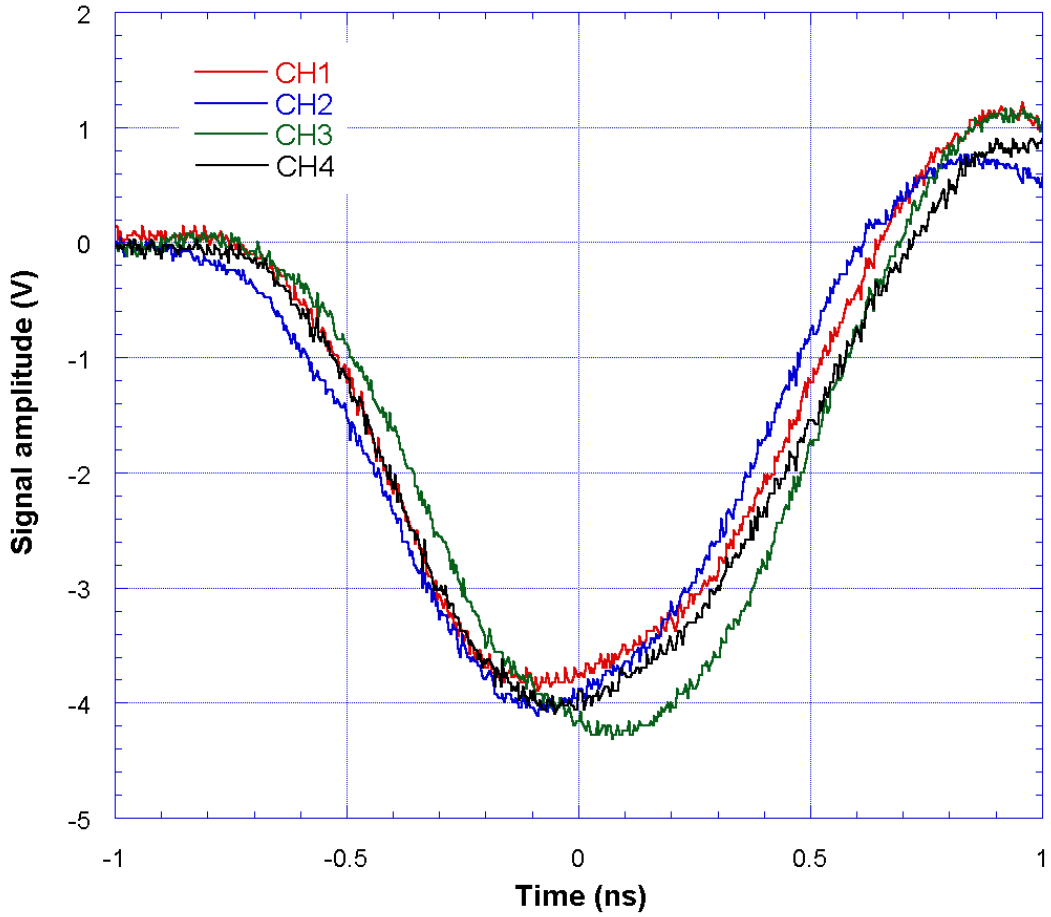


*Figure 6.24. Pulse output from the Alice PCB. Four pulses of approximately 4V amplitude are shown. Inter-channel timing skew can be seen at approximately 200ps.*

Figure 6.24 above shows the pulse outputs from the mark 1 PCB running at 10MHz into a 50Ω load. The pulses appear clean and symmetrical with a slight overshoot at the end of the pulse. Pulse widths are all approximately 850ps FWHM.

Three of the channels appear to be aligned extremely well temporally whilst channel 3 exhibits a -200ps skew. For large skew, this can be corrected manually by adjusting the channel digital delay. For low levels of skew (<500ps) the pulse can be adjusted by changing the trigger level of the driving amplifier.

The pulse amplitudes are all approximately 4V and originate from a low impedance source.

This means that the circuit will drive most types of laser diode directly without the need for pre-biasing the laser diode (which can lead to spontaneous emission from the laser diodes) or pulse amplification. An optical pulse from one of the output channels is shown below in Figure 6.25:

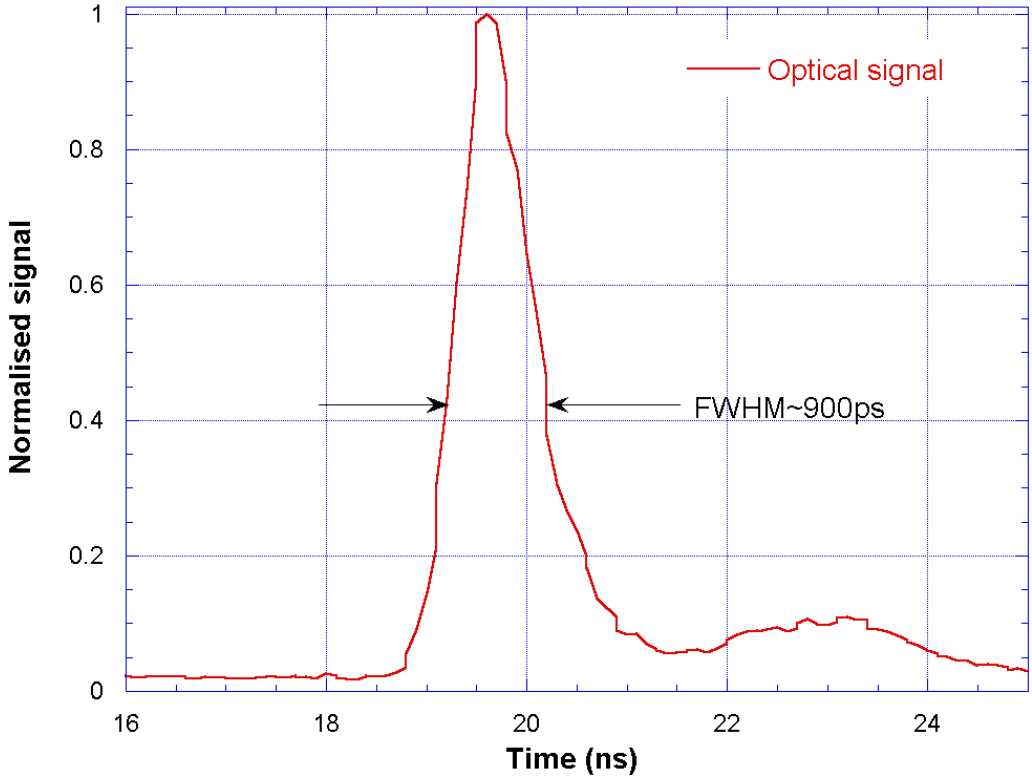


*Figure 6.25. Optical Laser pulse delivered by the Mark 1 Alice PCB. Clean, symmetrical shape and low afterpulsing. Pulse width is approximately 900ps.*

The pulse shown above is measured from the output of a laser diode used in the compact QKD system. The pulse looks clean with no spontaneous emission occurring before the pulse proper.

The pulse has a full width half maximum width of approximately 840ps which includes jitter from the driver circuitry and detection apparatus. A small afterpulse may be seen to the right of the trace. It is likely that this is due to a pulse reflection resulting from an impedance mismatch in the driver circuit. The amplitude of the after-pulse is small and would be further attenuated in a real system such that its contribution to errors or background count is negligible. Furthermore, any photons from the after pulse would arrive at the detector at least 2ns after the main pulse and would therefore arrive outside of the nominal 1.4ns timing gate in use by the detector system.

### *6.9.2 Laboratory tests*

The compact QKD system was thoroughly tested in the laboratory. Apart from functional testing of each component and sub-system, several key exchanges were performed under varying simulated conditions. For instance, atmospheric losses were simulated by placing neutral density filters in the optical path. Geometric losses were simulated by defocusing the Alice beam. The table below summarises the system tests:

| **Average photon number** | **Pulses sent** | **Pulses received** | **Distilled key (bits)** | **Final key rate (bits/s** | **QBER (%)** | **Calculated transmission loss** | **Range** |
|---|---|---|---|---|---|---|---|
| 0.1 | $7\times10^6$ | 692536 | 162140 | 937.23 | 5.74 | 16.35 | Lab |
| 0.1 | $7\times10^6$ | 19106 | 5376 | 168 | 4.37 | 31.15 | 40m |
| 0.1 | $70\times10^6$ | 930917 | 127840 | 998.75 | 7.78 | 27.38 | 80m |
| 0.1 | $70\times10^6$ | 1434103 | 259971 | 2015.3 | 6.76 | 24.3 | 80m |
| 0.1 | $7\times10^6$ | 109671 | 14663 | 1221.9 | 7.75 | 26.79 | 80m |
| 0.1 | $70\times10^6$ | 1039613 | 117600 | 890.91 | 8.32 | 27.75 | 80m |
| 0.1 | $70\times10^6$ | 130605 | 13370 | 297.11 | 8.45 | 28.74 | 1.2km |
| 0.1 | $60\times10^6$ | 396840 | 66550 | 496.64 | 7.06 | 29.55 | 1.2km |
| 0.1 | $10\times10^6$ | 68277 | 9329 | 233.23 | 7.6 | 30.3 | 1.2km |
| 0.63 | $300\times10^6$ | 139332 | 31804 | 365.56 | 11.6 | 38.99 | 1.2km |
| 1.2 | $500\times10^6$ | 480000 | 66550 | 554.58 | 7.1 | 38.58 | 1.2km |

*Table 6.1. Summary of the main parameters of the compact QKD system tests. Results are plotted and compared with the theoretical secure limits in Figure 6.26*

### *6.9.3 System tests and short range trials*

The compact system was tested over several ranges. Initial tests were conducted over a few metres in the laboratory with simulated attenuation loss provided by a combination of neutral density filters whilst beam defocusing provided geometric loss. Subsequent tests were conducted in building corridors in subdued daylight conditions over 40 and 80 metres. The final tests were conducted at the Pershore laser range facility described previously in chapter 5. The figure below shows some of the results from these tests with respect to a theoretical limit modelled under the GLLP assumptions modified with the compact system parameters.

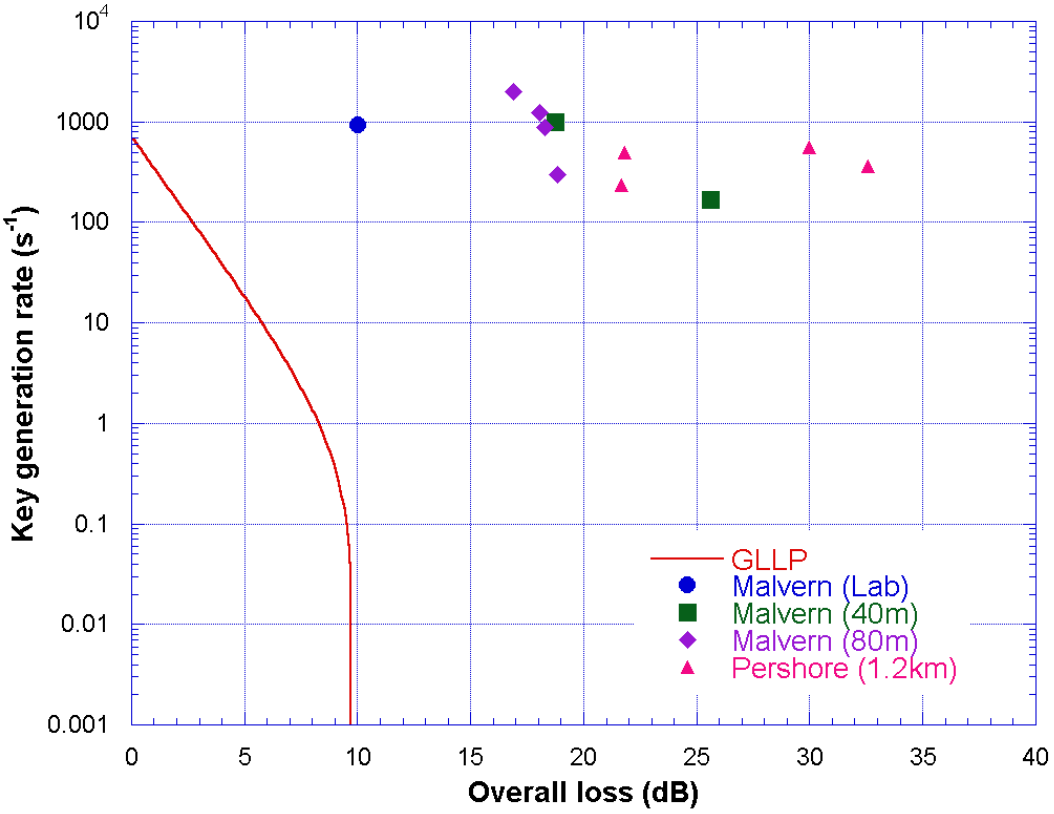


*Figure 6.26. Graph showing key exchange results compared to the (then) state of the art security analysis (GLLP).*

At first glance, these results seem fairly poor since all of the results are to the right of the red "GLLP" curve. This means that system losses are too high for the key exchanges to have rendered a secure key.

However, at this time the generally accepted wisdom was the use of average photon numbers of 0.1 photons per pulse would render the system secure. The tests above were performed under this rather naïve assumption. Furthermore, the high losses can be attributed to a number of technical issues:

The system used small aperture optics which were found to possess a high degree of aberration. Consequently, the optics were found to be far from diffraction limited, leading to difficulty in focussing which, in turn, led to large geometric losses, especially over longer ranges.

For the longer range trials at 1.2km, the optical transmission path runs very close to ground level which results in high levels of atmospheric turbulence. This can cause additional losses in terms of both geometric (beam spreading) loss and signal fading. This last factor can have serious effects in a QKD system since as the signal fades the key exchange rate can be reduced to zero. This effect becomes further factor in the high apparent losses due to the way in which the loss is calculated.

This incarnation of the system exchanges keys in a “block” mode. This means that key is exchanged in batches with each batch being preceded by a header which consists of timing information. If this header is not received or corrupted due to atmospheric effects, the whole block, including data, is discarded. Consequently the system loss appears to be much higher than the actual physical loss. A way around this would be to calculate the loss on the basis of “possible received” bits against actual received bits, thereby eliminating discarded blocks from the calculation. This method was used in calculating later results by recording the number of successful blocks transmitted.

### *6.9.4 BBN Technologies*

BBN Technologies Inc of Cambridge, Massachusetts managed the development of a Quantum Network under a DARPA project called QuIST. The network took the form of a fibre ring network in metropolitan Boston with nodes at Boston University, Harvard University and the BBN campus in Cambridge [1]. The network was designed to enable the distribution of quantum keys and the subsequent encryption of data transmitted over the network using those keys. It features standard security IPSEC protocols (internet protocol security) and AES encryption algorithms.

#### *6.9.4.1 System modifications*

The system designed for BBN was a duplicate of the short range system which has been described above. However, a few modifications were made to increase compatibility with the already extant Quantum network infrastructure:

The QKD system computers were repackaged in industry standard 1U 19” rack mounted casings which fitted directly into the BBN equipment racks. System cabling was rerouted to the computer front panels for ease of connection.

The BBN requirements necessitated some of the software modifications such that the system could operate in a master-slave mode. This was done primarily for compatibility with the BBN network management system. Two new programs, “Transmitterslave.exe” and “Receiverslave.exe” performed all the usual key exchange functions within the QKD system whilst control was maintained by two programs running on the BBN network management system (“Transmittermaster.exe” and “Receivermaster.exe”).

#### *6.9.4.2 System operation*

A short range free space QKD system was delivered to BBN at the end of March 2005 [17], [1] with the system unpacked, aligned and installed into the quantum network within an hour.

Later tests over 80m showed the system to be working satisfactorily with no re-alignment or adjustment due to transit required.

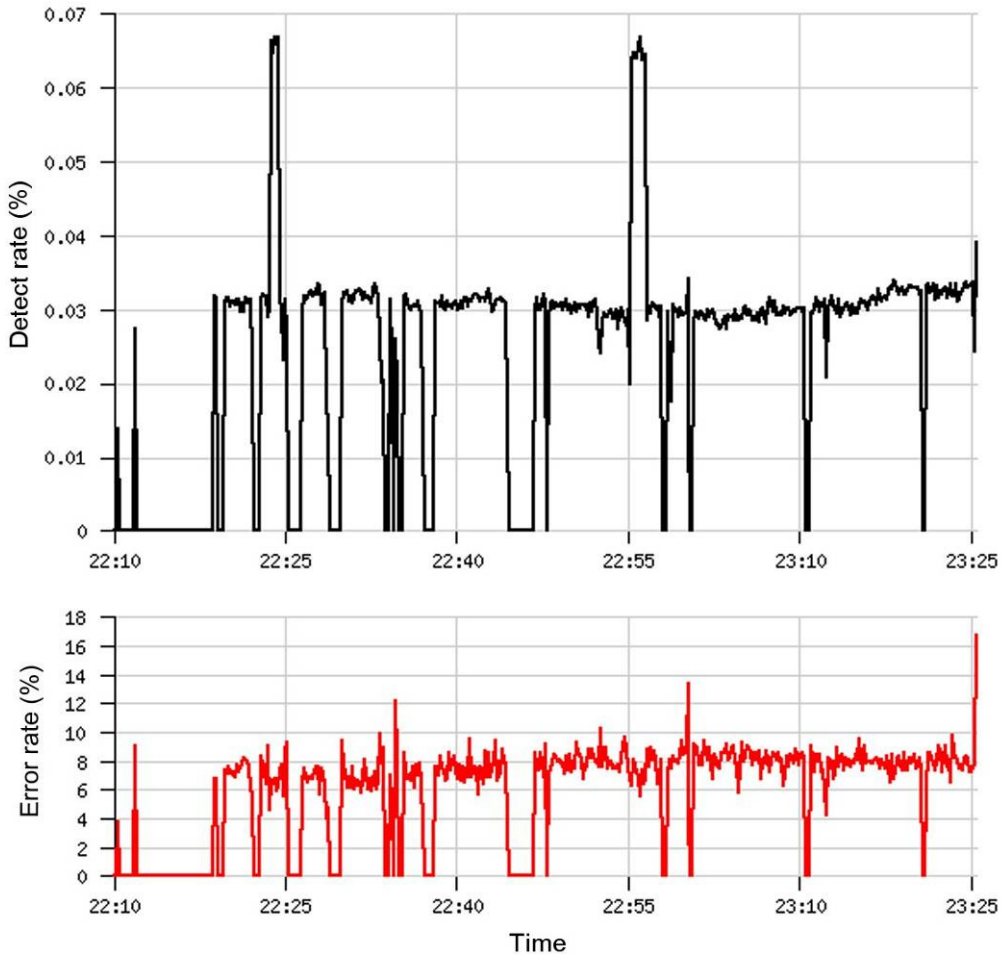


*Figure 6.27. First results from the BBN system. These results, kindly supplied by BBN technology, show the initial results from a key exchange experiment between buildings on the BBN campus in Cambridge Massachusetts, U.S.A.*

The figure above, kindly supplied by BBN, shows some results from an initial experiment conducted between two buildings. The plots show the first hour and fifteen minutes of operation using test data. For most of this time the system was operating through two closed windows in steady rain. Several of the artefacts are due to room lights being turned on (error rate spikes) and windows being opened by the operators (detect rate increases). The results are encouraging and the system appears to be stable. The rather high error rate was attributed by BBN to the effects of a flood light reflecting from the window in front of the Alice terminal and causing increased background counts in the Bob receiver. The system was subsequently operated continuously as part of the DARPA quantum network.

### *6.9.5 Long-range trials at the Canary Islands*

This section describes the participation of the QinetiQ team in the long distance free-space QKD experiments conducted between the islands of La Palma and Tenerife in the Canary Islands during June 2006. The work was funded by ESA under contract No. 18805/04/NL/HE, QIPS: Quantum Information and Quantum Physics in Space: Experimental Evaluation.

#### *6.9.5.1 Background*

The idea of performing QKD to satellites has been mentioned in nearly every published free-space QKD paper since 1995 (for example, see [18] - [21]). In 2002, the European Space Agency (ESA) commissioned a short study called QSPACE (contract no. 16441/02/NL/SFe) under its General Studies Programme. The aim of this project was to "investigate and review the emerging field of Quantum Communications with particular reference to Space Applications". By the summer of 2003, two final reports had been delivered (for various reasons the study was split between two separate groups). Whilst both studies agreed on several likely scenarios for future research in this area, one of these reports [22], detailed a feasibility experiment between astronomical telescopes located at observatories on the Canary Islands. .


*Figure 6.28. The proposed trials range in the Canary Islands. Alice is located at the Observatorio del Roque de Los Muchachos, whilst Bob is located at the Observatorio del Teide on Tenerife.*

The proposed experiment was to perform a demonstration of QKD between the locations shown below, which constitutes a range of 144km

A successful key exchange over this distance would prove the feasibility of operation to high altitude aircraft and balloon platforms, low earth orbit, and, perhaps, to satellites in the geostationary ring. Moreover it would extend operational distances of cryptographic key distribution systems to really practical ranges, for example, between major cities.

The trials location was chosen for the following reasons:

- ESA have used this location as a trial site for the SILEX optical communications demonstrator prior to space validation experiments from the Artemis satellite.
- There exists a clear horizontal line of sight of 144km, above the first inversion layer (cloud line), with prevailing good clear weather.
- The presence of infrastructure (power, accommodation, communications) at both ends of the range.

#### *6.9.5.2 Experimental set up*

It should be made clear, here, that the experimental infrastructure was put in place by the Munich (Tobias Schmitt-Manderbach and colleagues) and Vienna (Rupert Ursin and colleagues) teams. The QinetiQ equipment was air-freighted to the trials location allowing ample time for any repairs, setting up and testing. Trials personnel followed one week later, with two specialists being deployed to each location.

Alice (operated by David Benton and the author) was located in a Portakabin at the Nordic Optical Telescope which is situated at the Observatorio del Roque de Los Muchachos on La Palma. The telescope is the highest at the observatory and is some 200 feet below the summit of the mountain. It is also the only telescope with a view of the island of Tenerife.

The various Alice modules were fibre coupled into a purpose built, steerable, refracting telescope, with an objective lens some 5 inches in diameter. The telescope was situated externally and consisted of two channels, one each for data and tracking. A photograph of the telescope is shown below in Figure 6.29.

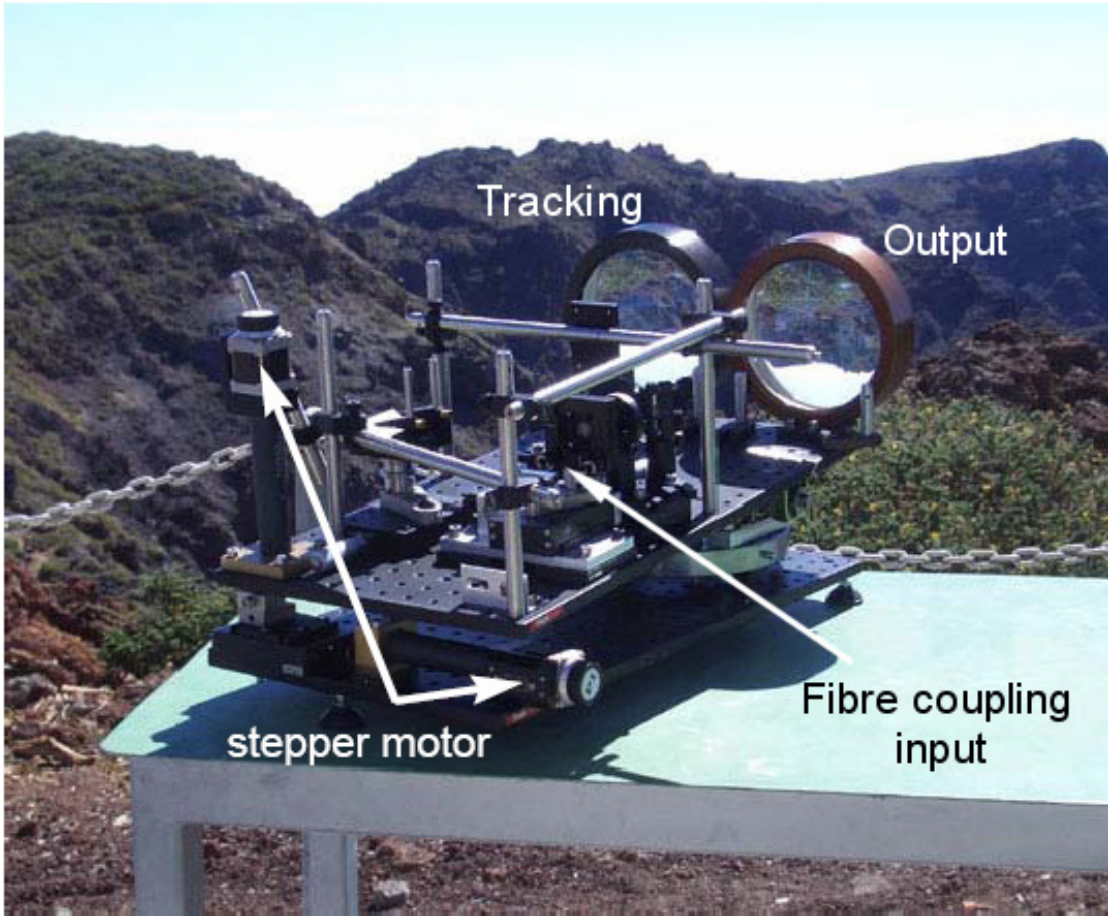


*Figure 6.29. Alice output telescope (showing stepper motors and the two output lenses).The telescope was situated externally next to the Nordic Optical Telescope and coupled by single mode fibre to the Alice modules.*

Bob (Paul Tapster and David Taylor) was located inside the telescope building of the Optical Ground Station owned by the European Space Agency.

The telescope is a 1m Ritchey-Chrétien/Coudé telescope supported by an English mount inside a dome 12.5m in diameter. The OGS forms part of the telescope facilities of the Observatorio del Teide on the island of Tenerife. Both observatories form part of the European Northern Observatory and are administered by the Instituto de Astrofisica de Canarias (IAC).

The Bob receiver was constructed on an optical bench inside the Coudé room (the room below the telescope dome where the so-called Coudé focus is situated). The idea of a Coudé focus is that the observing instruments may be kept stationary whilst the telescope is moved to any position. This is ideal for the Quantum Cryptographic receiver used in these trials; moreover, this telescope has already been proven in optical communication experiments to space-based platforms.

A photograph of the Bob module is shown below in Figure 6.30. The Bob used in these experiments was built by the team of John Rarity at the University of Bristol and, whilst typical of the "generic" type Bob, was significantly larger than the usual sized modules used in the QinetiQ system. The main reason for this was that the Coudé focus of the optical ground station has a large F number (~F#32). To maintain optimum efficiency and to gain maximum advantage from the large diameter of the collecting telescope it was necessary to construct an optically compatible Bob system.

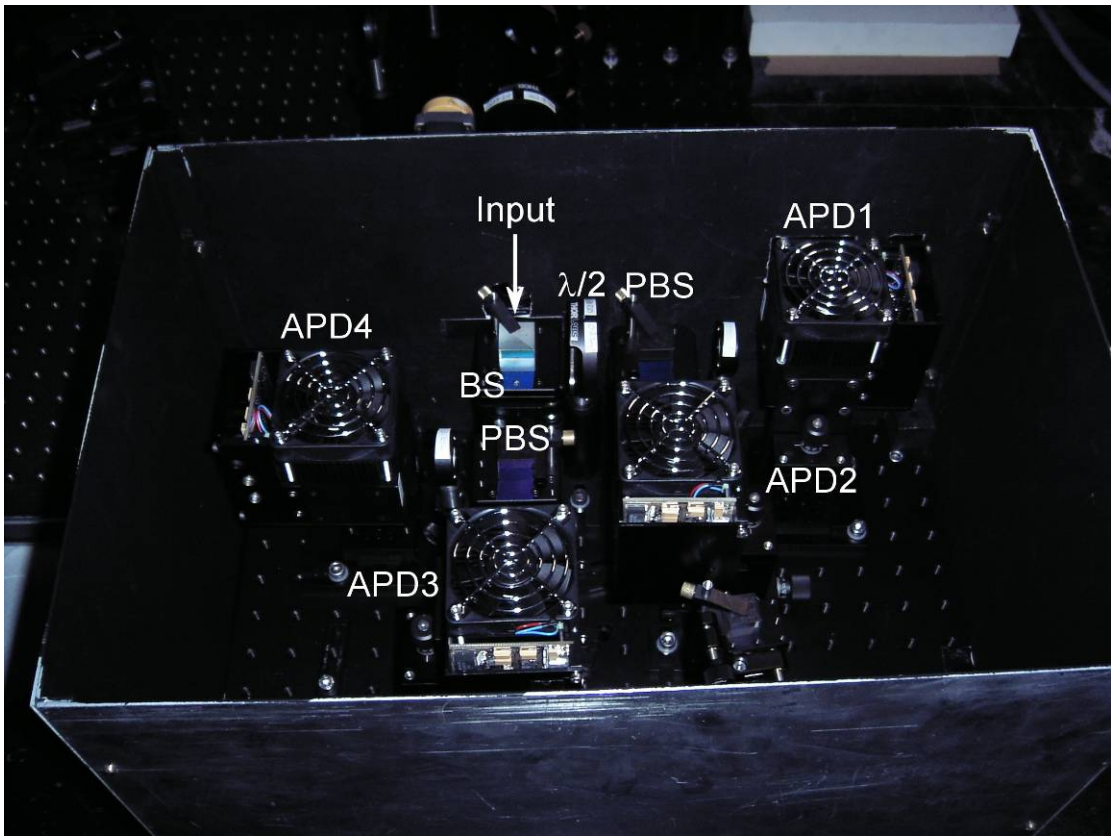


*Figure 6.30. Photograph of the Bob receiver used on Tenerife (BS-beam splitter, PBS-polarising beam splitter, APD-avalanche photodiode, λ/2-half-wave plate).*

#### *6.9.5.3 Enabling modifications to the QinetiQ Alice and software.*

The QinetiQ system required some modification in order to be able to work with the existing trials infrastructure.

***Movement of the operating wavelength to 850nm.***

By agreement the wavelength of operation for all the teams at the trial was 850nm. Advantages to be gained are that atmospheric transmission is slightly better than the customary QinetiQ 630-670nm wavelength, whilst the sensitivity of the single photon detectors is marginally better. The use of this wavelength required extensive modifications to the Alice head including new laser diodes and specific wavelength based optics.

***Installation of a fibre coupling mechanism to Alice.***

This was an essential modification because the output telescope at the ALICE station was designed to be fibre coupled. This allowed for ease of connection to the telescope and made changing from one system to another very easy. However, propagation through fibre can seriously perturb the well defined polarisation directions, leading to the output from the telescope being elliptically polarised.

A system of polarisation rotating elements were installed in the Alice module to allow pre-compensation of the polarisation before the output of the system. This allowed the operators to "tune" the polarisation accurately to compensate for the 10m of optical fibre between module and output telescope. Using this method the operators were able to "tune" the polarisation to within 3% of optimum.

***Installation of an additional time tagging card at Bob.***

This had the effect of doubling the throughput of the system and increasing the signal to noise ratio by 3dB. Incorporation of this card required significant work to amend software based on a single time tagging card. A further calibration stage was required to ensure that both cards, whilst operating independently, were referenced to the same starting point. This allowed events registered in different cards to be compared and integrated into a single data set.

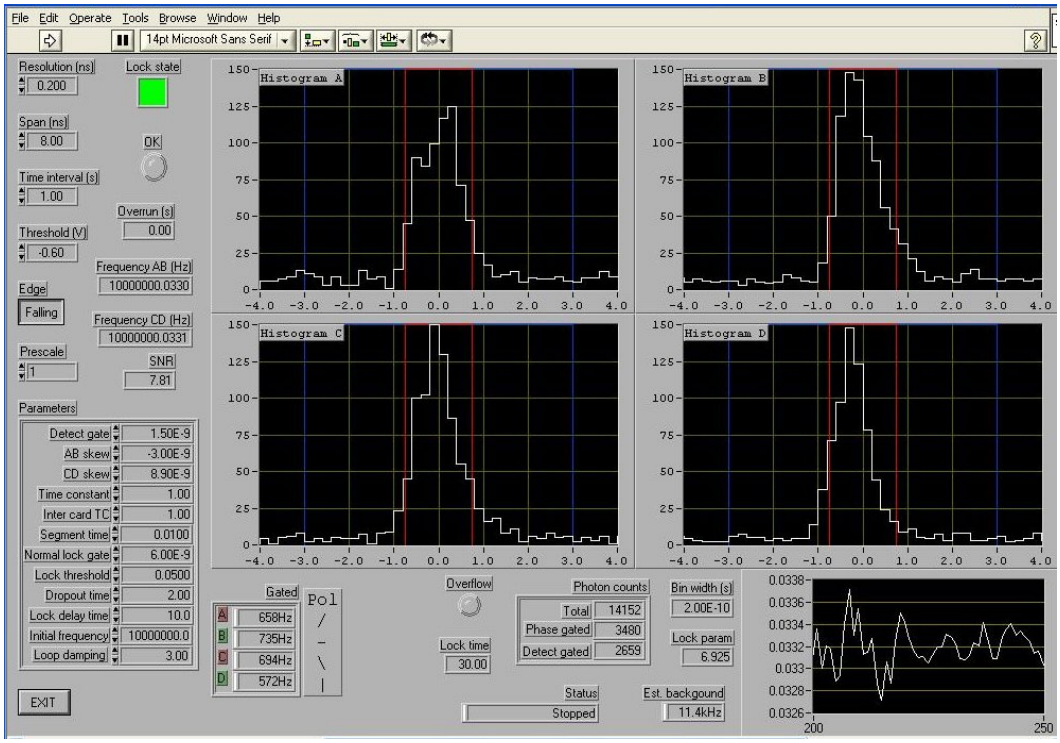


*Figure 6.31. Screenshot of the diagnostic programme "PLLtestquad.vi" showing histograms of the four detection channels locked to 1.4ns detection gates.*

***Pulsed alignment laser.***

When the ALICE system sends data to the Bob terminal, it transmits that data in the form of a "block". Each "block" of data is preceded by a header which contains information that enables the system to remain accurately synchronised.

If this header information is lost, for example, due to extreme transmission losses, then the whole packet of data is lost. If, however, the header information can be sent using a brighter source, there is a higher likelihood of the header data reaching Bob. This increases the chances of maintaining synchronisation of the system and even if most of the data (at normal brightness) is lost, the data which does reach Bob is still valid for the purposes of a key exchange. Thus the system can be made more robust and efficient by making the headers brighter.

This idea was implemented by providing an additional fast pulsing circuit for the bright alignment laser (described above), thus when the headers were sent the software was programmed to pulse the four data lasers and the alignment laser simultaneously. During the data part of the block, however, the alignment source was inactivated thus preserving the low average photon number for the data segment of the blocks.

In this way the system was made much more robust to transmission losses. A further related development was to make the header segment of the data packets variable in length in order to again increase the probability of the header arriving intact at the receiver.

#### *6.9.5.4 Experimental operations*

The experimental schedule required that several sub-systems be installed and working before QKD experiments could take place.

***Random numbers:***

All random numbers used at the Canary Islands were generated in-situ by the RNG described in section 6.3 of this chapter. For the packet mode experiments, the random numbers were generated locally and stored on the Alice controller PC hard-drives as binary files. For continuous QKD, the RNG was integrated into the QKD software and was capable of providing real time random numbers at an adequate rate for operation at 10MHz.

***Pointing and tracking:***

The first subsystem to be set up and tested was the pointing and tracking system. This subsystem is critical to the efficient working of a free-space optical system operating beyond a few kilometres. The reason for this is that both terminals appear to move with respect to each other.

This movement is caused by atmospheric turbulence and is directly related to propagation distance, temperature gradients and air movements in the transmission path (see chapter 3 for a discussion of atmospheric transmission). The system consisted of laser beacons and associated CCD cameras boresighted to the data channels. This arrangement provided an error signal to control a set of motorised micrometers in the case of Alice, and the OGS pointing system in the case of Bob. The system was controlled by a pair of personal computers running custom written LabVIEW software designed to keep the two telescopes pointing at each other. This arrangement allowed compensation of atmospheric induced beam wander to be controlled in real time.

The pointing and tracking was considered a vital part of the experimental set-up as, during earlier tests, vertical deviations of up to 100m were recorded during experimental operations. A previous inactive alignment system was only capable of operating stably for around 30 minutes at a time, whereas the latest active system enabled the maintenance of alignment for several hours. Figure 6.32 below shows typical behaviour of the tracking system.

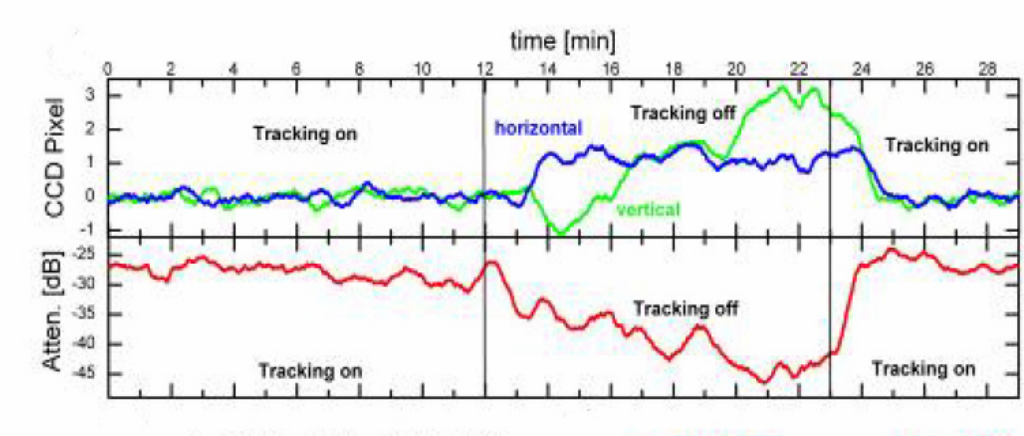


*Figure 6.32. Tracking and pointing behaviour over 30 minutes (the blue and green lines show the apparent deviation of the tracking laser spot on the CCD image element, the red line shows the changes in optical transmission as a result of these deviations (Image: LMU/Uni' Vienna).*

One can see that as a result of atmospheric turbulence, the channel losses can vary between 25 and 45dB. The problem here is twofold; (1) a 20dB dynamic range on the optical signal is difficult to deal with during signal processing and (2) at >32dB of channel loss, the system is essentially crippled.

***Optical transmission measurement***

The second phase of the trials was designed to allow long term measurements to be made of the optical transmission of the range whilst under full tracking control. Facilities were also included to allow spot (instantaneous) measurements to be made throughout the trials duration.

In addition, the QinetiQ system provided enough real time information to be able to calculate the system transmission losses for each key exchange.

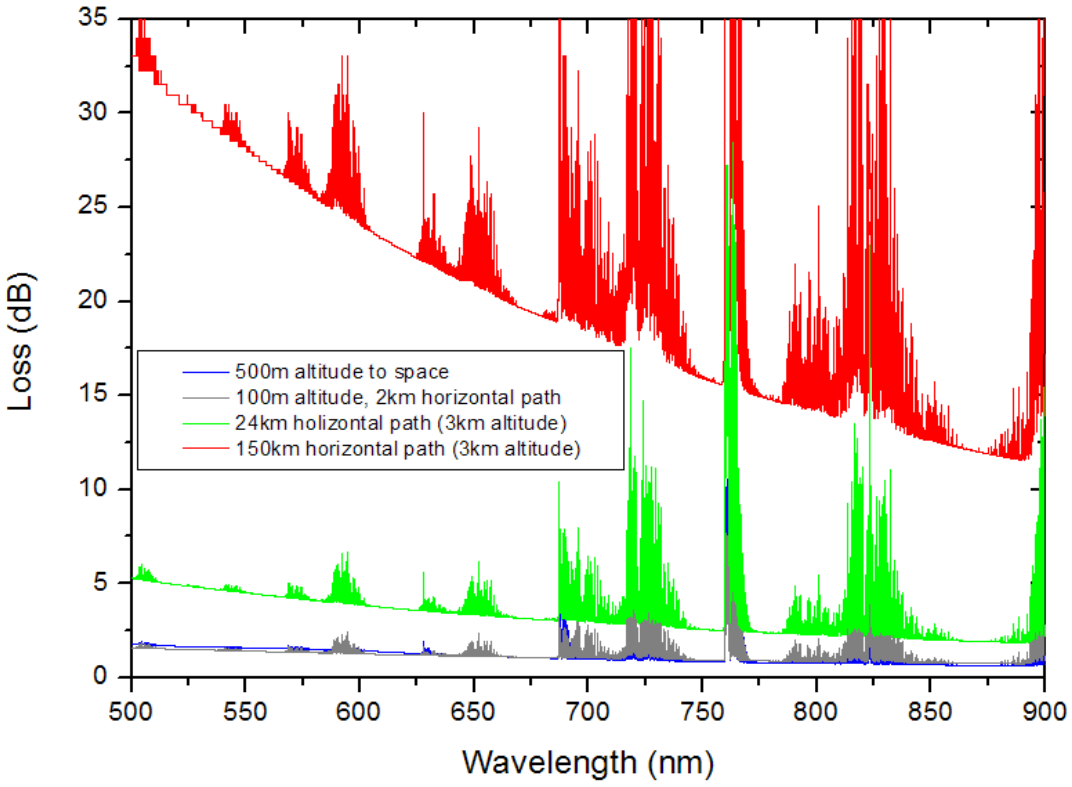


*Figure 6.33. Modelled losses for different transmission scenarios. The trace in red is a simulation of the 144km experiment in the Canaries. (Courtesy of Dr. David Taylor).*

Modelled theory (using MODTRAN) gives a figure of approximately 12dB loss at 850nm for a 150km horizontal path. A plot of modelled channel attenuation loss is shown above in Figure 6.33. This figure does not include contributions from turbulence effects or optical losses within each system. Also shown in the figure are models of three other scenarios including a transmit path to space from a ground station located at 500m above sea level. The transmission losses here are comparable with a 2km horizontal transmission path at 100m altitude. Both of these scenarios offer significantly lower loss than either the 24 or 144km predictions for atmospheric attenuation.

In addition to absorption and scattering, one might expect substantial geometric losses due to beam spreading and beam wander arising as a result of atmospheric turbulence, scatter and diffraction.

The amount of each effect depends on the physical scale of the turbulent cells along the transmission path with large scale turbulent cells giving rise to beam wander whilst smaller scale cells give rise to beam spreading and "breathing".

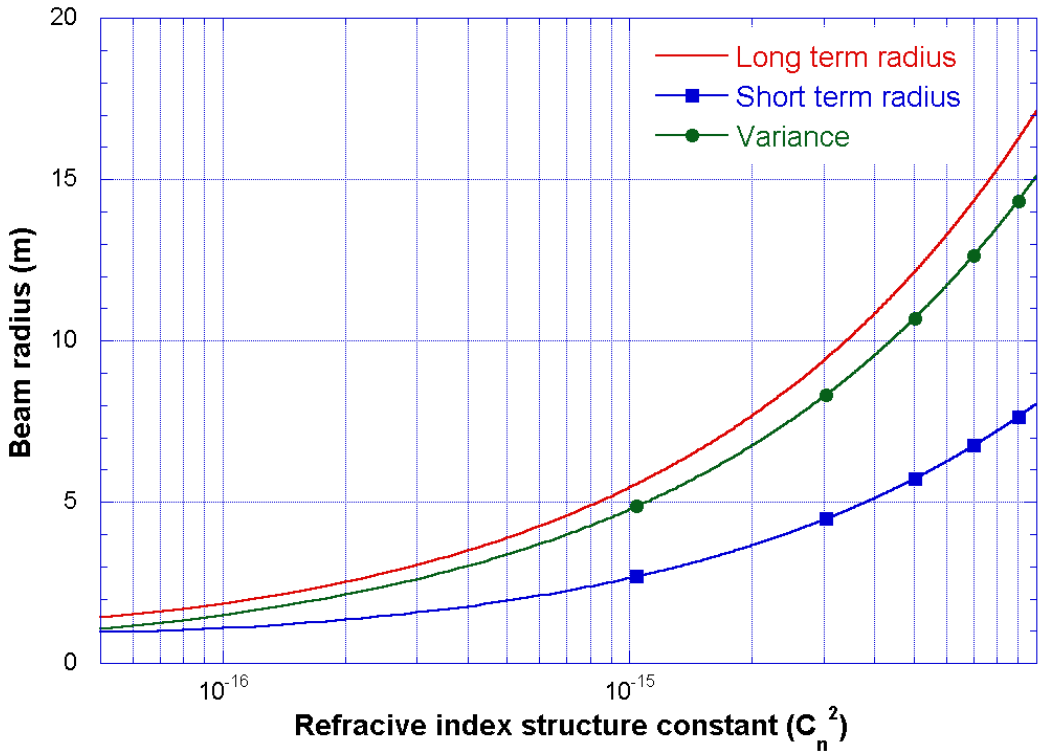


*Figure 6.34. Short term spreading and long term beam wander estimation for a 100mm (initial) diameter optical beam at 850nm wavelength over a range of 144km.*

One can estimate the geometric losses by modelling the effects of turbulence. Figure 6.34 above uses the theory of Andrews and Philips [26] to predict the turbulence induced beam wander under a weak turbulence approximation using the experimental parameters given in [24] (i.e. 100mm transmit diameter, diffraction limited, 850nm beam).

The theory predicts short term beam radii ranging from approximately 1 to 4.8 metres whilst long term beam sizes range from 2 to approximately 10m, depending on the strength of the turbulence along the transmission path (here, values of $C_n^2$ estimated at the time of $1.198\times10^{-16}$ and $3.4936\times10^{-17}$ are used as best and worse cases). With a receiver telescope aperture of 1m, the geometric losses due to short term spreading then range from approximately 7 to 20dB. A further 10dB loss is estimated by Schmitt-Manderbach et al to take account of the transmit (-1dB), receive (-3dB) optics and receiver SPAD efficiency (-6dB). Table 6.2. (below) shows an estimate of losses from various sources:

| Component | Estimated loss | Comments |
|---|---|---|
| Attenuation and scattering | -12dB | MODTRAN modelling |
| Geometric | -7 to -20dB | Depends on $C_n^2$ [26] |
| Alice optics | -1dB | Estimated at 850nm |
| Bob optics | -3dB | Estimated at 850nm |
| SPAD efficiency | -6dB | 25% efficiency estimate |
| Total | -29 to -42dB | -34 to -44dB measured |

*Table 6.2. Estimation of free-space channel losses for the Canary Island experiments.*

It appears that predicted losses agree closely with measured values. Clearly the largest contribution to the loss is from atmospheric effects. This loss also varies over several timescales and depends on the prevailing weather conditions at the time. Long term beam wander is not a cause of loss as such but will tend to cause signal loss when the beam wanders away from the receiver aperture. This can be compensated with an active pointing system with sufficient bandwidth.

The final phase of the trial containing the quantum cryptography experiments then commenced. LMU/Vienna conducted experiments first (see [24] and [25] for full details of these experiments) with QinetiQ being allotted time on the last four nights of the trial. However, due to unseasonably bad weather, a transmission path was unavailable during the last two nights and only partially available on the second night. A screenshot of the observatory weather station data output is shown below in Figure 6.35. Attention is drawn to the readings for Dew point, Humidity and Temperature. At this time the NOT telescope dome had closed and was inside a cloud.

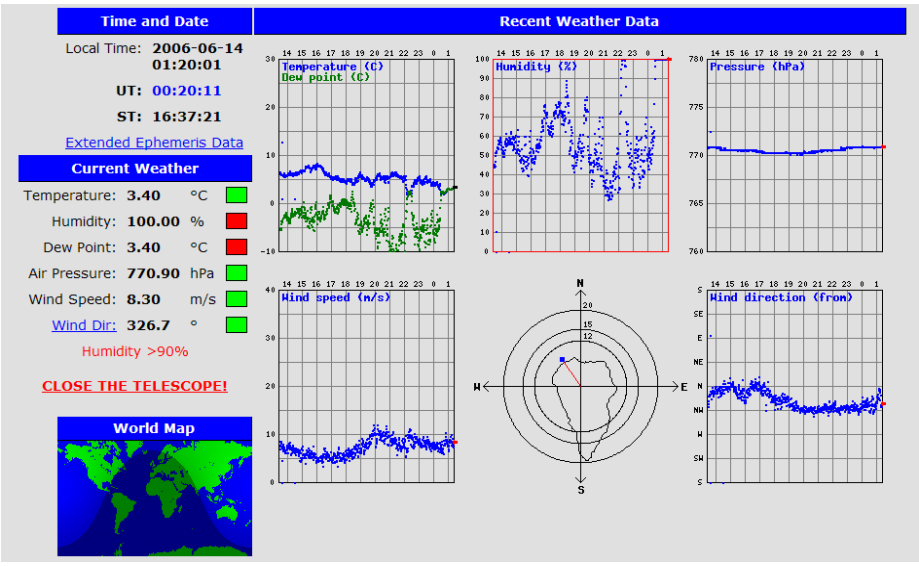


*Figure 6.35. Weather station data, NOT 01.20am 14/06/2006. Note the humidity and dew point readings indicating the presence of cloud.*

#### *6.9.5.5 Results and discussion*

A list of experimental goals is shown below in Table 6.3.

| | **Goal** | **Accomplished** |
|---|---|---|
| 1 | Single photon transmission | YES |
| 2 | Remote control B to A | YES |
| 3 | Remote control A to B | YES |
| 4 | Demonstration of 144km key exchange | YES |
| 5 | QKD in packet mode | YES |
| 6 | QKD in continuous mode | NO |
| 7 | Real time random numbers | NO |

*Table 6.3. Experimental goals for the QinetiQ team.*

Despite the bad weather, the trials team were able to accomplish most of the experimental goals:

***Goal 1*** (Single photon transmission) was accomplished within seconds of connecting the Alice to the output telescope on the first night of operation, mainly due to the excellent alignment system provided by the Viennese contingent. Due to a local computer malfunction, the adjustment of Alice pulse timing and polarisation compensation was achieved over the internet link using the Tenerife receiver rather than with local equipment.

***Goal 2 and 3*** (Remote control A to B and B to A) were accomplished during the succeeding key exchanges. The communication system utilised throughout the trials was an ordinary internet connection running at a nominal 10Mbits/s. The team was able to run a voice over IP (VOIP) connection for communications as well as the TCP/IP (a normal internet communications protocol) connection required for the classical communication channel required by the experiment. Remote control was achieved from both terminals using the freeware program VNC. No further software or hardware was required for this goal.

***Goal 3*** (Demonstration of 144km key exchange) was achieved on the second night once transmission was demonstrated at the single photon level. This was achieved at 12.05 am on the morning of the 13/06/2006.

***Goal 4 and 5*** (QKD in packet mode) was achieved over a set of 10 key exchanges. A table of key exchange results is shown below:

| Serial | Average photon number | Received (Bits) | Final Key (Bits) | Bit rate (Bits/s) | QBER (%) | Measured transmission loss (dB) |
|---|---|---|---|---|---|---|
| 1 | 4 | 12367 | 2187 | 43.4 | 5 | 34.85 |
| 2 | 4 | 29660 | 6237 | 101 | 5.4 | 36.83 |
| 3 | 4 | 64989 | 14574 | 157 | 5.4 | 36.44 |
| 4 | 2 | 8303 | 680 | 6.94 | 8.7 | 41.11 |
| 5 | 2 | 30115 | 4384 | 46.8 | 7.1 | 39.27 |
| 6 | 1.3 | 9717 | 232 | 2.1 | 9.99 | 41.88 |
| 7 | 1.3 | 21584 | 800 | 8.5 | 9.78 | 41.43 |
| 8 | 1.3 | 13947 | 1888 | 17.3 | 7.76 | 42.07 |
| 9 | 1.3 | 6499 | 194 | 1.82 | 9.6 | 43.17 |
| 10 | 1.3 | 6000 | 1534 | 10.4 | 10.19 | 43.99 |

*Table 6.4. Summary of results from key exchange experiments on the night of the 13-14th June 2006.*

Varying degrees of success were achieved as the team ran through several software and hardware configurations in an effort to determine the optimum combination of settings. With reference to the channel loss, here calculated by analysing the number of possible detections (i.e. those detections arising from valid blocks of data. See 1.6.5.4 above) against the number of actual detections, it is clear that as the experiment progressed, increasing levels of channel attenuation were experienced which reduced the likelihood of successful transmission. The table below shows the system parameters for the Canary Islands experiment. The parameters are identical to those reported by Schmitt-Manderbach et al except that the QinetiQ system was able to use a significantly narrower timing gate at the Bob receiver. This resulted in a reduced background count without impacting the signal to noise ratio unduly.

| **Alice optical loss (dB)** | **Bob optical loss (dB)** | **Detector efficiency (%)** | **Background probability per time slot** | **Detector error (%)** | **Time gate (ns)** |
|---|---|---|---|---|---|
| 1 | 3 | 0.25 (-6dB) | $0.4\times10^{-6}$ per detector | 3 | 1.4 |

*Table 6.5. Experimental parameters for the Canary island experiments.*

A comparison of results with the relevant theoretical security limits is shown below in Figure 6.36:

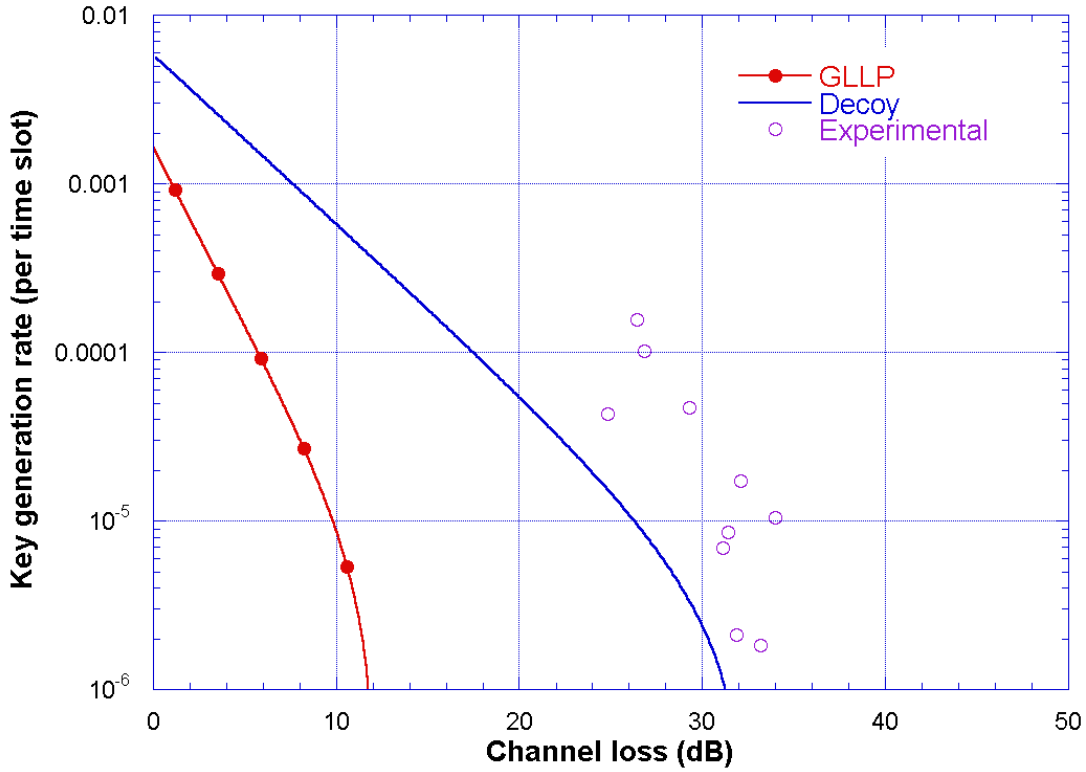


*Figure 6.36. Key exchange rates against channel loss for experimental results at the Canary islands with respect to theoretical limits given by GLLP($\mu=\eta$) [27] and Decoy state($\mu$=0.3) [28] analysis of the system parameters given in [24] and shown in* ***Error! Reference source not found.****.*

The figure above shows the set of ten key exchanges listed in Table 6.4. plotted with respect to two theoretical curves which have been modelled according to the experimental settings shown in Table 6.5. The curves represent the limits for secure key exchanges under two regimes. The dotted curve represents the upper limit for key generation using the so-called GLLP analysis of QKD security with the average photon number, $\mu$, set equal to the transmission efficiency, $\eta$.

The solid curve shows the limit under the same conditions when using a Decoy state regime as analysed by Lo et al in [28].

The graph in the figure is plotted to show only actual channel loss, i.e. any optics losses in the system are counted as system losses and removed from the plot (4dB in this case). This accounts for the rather low initial key generation rates and somewhat reduced maximum total losses.

The reason for plotting the limits in this way is that it allows easier comparison with other types of system, for instance the fibre based systems analysed in [28].

The experimental results (plotted as circles) are clearly beyond the limits of secure key distribution, both in terms of channel losses and average photon number, particularly as

these results are generated using a standard BB84 protocol. From this point of view the experiment was disappointing. However, in terms of hardware development, the system performed superbly with key exchange taking place within an hour of setting up the experiment. The fact that any exchange at all was achieved with total system losses approaching 44dB is an achievement in itself.

System set up and operation was made simple by the use of several diagnostic programs.

It is most unfortunate that uncharacteristically inclement weather prevented further experimentation and the intended implementation of a Decoy state protocol and continuous key exchange.

Some might argue that in a free-space transmission situation, one always has a line of sight between the QKD terminals and thus can physically spot potential eavesdroppers, however, this experiment was merely a feasibility experiment. In real systems, such as ground to space and space to space a clear line of sight may not always exist to monitor for the physical presence of eavesdroppers, and anyway this is a specious argument since the whole point of the experiment was to validate the theory.

### 6.10 Summary and conclusion

This chapter has described the initial development of a lightweight compact and portable free-space QKD system, against the background of general improvement in QKD technologies around the world. The main problems addressed during this phase were reliability and size of components and functionality of the electronics and software.

Additionally, several trials and demonstrations have been described with reference to the (then) current security proofs for QKD systems. The chapter culminates in the participation in a truly ambitious proof of principle experiment conducted at high altitude between the Islands of La Palma and Tenerife in the Canary Islands, the results of which imply that QKD to low earth orbit (LEO) and, perhaps, to geostationary orbit GEO is both feasible and practical.


*Figure 6.37.The night view from the QKD transmitter telescope at the Nordic Optical Telescope on La Palma looking toward Tenerife. The green tracking beam is aimed toward the Optical ground station (OGS). One can also see the return beam as a blob of light with mount Teide to the right. (Photograph courtesy of David Benton).*

## 6.11 Chapter 6 references


[1] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, H. Yeh, "Current status of the DARPA Quantum Network", SPIE Quantum Information and Computation III, 28 March – 1 April, 2005, Orlando, Florida, Proc. SPIE Vol. 5815, (2005).

[2] C. H. Bennet and G. Brassard, "Quantum cryptography: Public key cryptography and coin tossing", Proceedings of the International conference on computers, systems and signal processing, Bangalore, India, December 10-12 1984, pp. 175 – 179, (1984).

[3] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P.M. Gorman, P.R. Tapster, and J.G. Rarity, "Quantum cryptography: A step towards global key distribution", Nature **419**, 450, (2002).

[4] J. Franson, and B. Jacobs, "Quantum cryptography in free-space", Optics Letters **21**, 1854–1856, (1996).

[5] C. E. Shannon, "A mathematical theory of communication", The Bell System Technical Journal, **27**, 379–423, 623–656, (1948).

[6] Federal Information Processing Standards Publication, FIPS PUB 140-2, "Security Requirements for Cryptographic Modules", (2002).

[7] The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness. URL http://www.stat.fsu.edu/pub/diehard/, (1995).

[8] P. R. Tapster and P. M Gorman, "Apparatus and method for generating random numbers", United Kingdom patent filing, Patent no.0603523.2, (2007).

[9] M. Fiorentino, C. Santori, S. M. Spillane, and R. G. Beausoleil & W. J. Munro, Secure self-calibrating quantum random-bit generator, Physical Review A **75**, 032334 (2007).

[10] B. Jun and P. Kocher, The Intel® Random Number Generator, Cryptography Research, inc. White paper prepared for Intel Corporation, (April 22, 1999).

[11] IDQuantique white paper: “Quantis Quantum Random Number Generator”, URL:http://www.idquantique.com/images/stories/PDF/quantisrandomgenerator/quantis-whitepaper.pdf, (2010).

[12] Zetex Application Note 8, Issue 2, “The ZTX415 Avalanche Mode Transistor”, (January 1996).

[13] Millman and Taub, “Pulse, Digital and Switching waveforms”, McGraw-Hill,. (Library of congress catalogue no. 64-66293). p96, p759, (1965).

[14] Hewlett-Packard Application note AN918, “Pulse and waveform generation with step recovery diodes”, (1984).

[15] J. S. Lee and C. Nguyen, “Uniplanar picosecond pulse generator using step recovery diode”, Electronics Letters, **37**, 8, 504-506, (2001).

[16] C-MAC Corporation CFPO-4: High Stability OCXO datasheet, (1999).

[17] P.R. Tapster P.M. Gorman D.M. Benton, D.M. Taylor and B.S. Lowans, “Developments towards practical free-space quantum cryptography”, SPIE Quantum Information and Computation III, 28 March – 1 April, 2005, Orlando, Florida, Proc. SPIE Vol. 5815, (2005).

[18] J. Franson, and B.Jacobs, “Quantum cryptography in free-space”, Optics Letters **21**, 1854–1856, (1996).

[19] W.T. Buttler, R.J. Hughes, P.G. Kwiat, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, and C.M. Simmons, “Free space quantum key distribution”, Physical Review A **57**, 2379–2382, (1998).

[20] R.J. Hughes, W.T. Buttler, P.G. Kwiat, S.K., Lamoreaux, G.L. Morgan, J.E. Nordholt, and C.G. Peterson, “Quantum Cryptography For Secure Satellite Communications”, IEEE Aerospace 2000 Conference, Big Sky, Montana (14-25/3/2000).

[21] J.G. Rarity, P.R. Tapster, P.M. Gorman and P. Knight, “Ground to satellite secure key exchange using quantum cryptography”, New Journal of Physics, **4,** 82.1–82.21, (2002).

[22] J.G. Rarity, Quantum Communications in Space, Executive summary, ESTEC 16441/02/NL/Sfe, (2003).

[23] M. Fürst, T. Schmitt-Manderbach, J.G. Rarity, R. Ursin, H. Weier and H. Weinfurter, "Quantum Information and quantum Physics in Space Experimental Evaluation", ESA contract No.18805/04/NL/HE QIPS, Technical Note 5: "Experimental evaluation of proof-of-concept demonstrator", (2005).

[24] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J.G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km", Phys. Rev. Lett. **98**, 010504, (2007).

[25] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J.G. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter & A. Zeilinger, Entanglement-based quantum communication over 144 km, Nature Physics **3**, 481 – 486, (2007).

[26] L.C. Andrews and R.L. Phillips, "Laser beam propagation through random media", SPIE press ISBN 0-8194-2787-X, (1998).

[27] D. Gottesman, H-K. Lo, N. Lütkenhaus, J. Preskill, "Security of quantum key distribution with imperfect devices", Quant.Inf.Comput., **5,** 325-360, (2004).

[28] H-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution", Phys. Rev. Lett. **94**, 230504, (2005).

# Chapter 7 - Further research- Daylight operation, 2006 - 2008

## 7.1 Introduction

In the previous chapter, the development of a compact QKD system was described from initial design through to working system. Like many systems operating at the time, many of the fundamental problems of design and construction had been solved, or at least, understood. What remained, however, was the so-called "valley of death" or in other words the gulf between the working prototype and the productionised version of a final product. Whilst there were commercial systems available they were fibre-based point to point systems usually operating over dark fibre (i.e. fibre which carries no other signals). For free-space QKD there was still much to be done despite the demonstration of 144km decoy state and entanglement based key distribution discussed in the previous chapter. Specifically, many free-space systems were unable to operate in true daylight conditions. Furthermore, many systems still required a team of operators, usually highly qualified, to coax them into operation. In addition, it was becoming clear that systems yielding a few bits per second of final key were not practical. In light of this most of the active QKD teams were in a process of continuous development of their systems as was revealed (and still is) by the published literature. For QinetiQ the main themes for system development over the next few years of free-space QKD were to be:

- Electronics enhancement
- Daylight operation
- General development work

This chapter will discuss some of these issues and show how some of the problems were solved, given that by this time the compact system was approaching five years old.

## 7.2 Electronics enhancement[11]

In the previous chapter a so-called Mark 1 Alice driver was developed which co-located all of the components and functions required for operation of a QKD transmitter on one professional quality printed circuit board (PCB). With the benefit of trials experience it was decided to improve the functionality of the design with a second iteration focussing on the following areas:

- Automated adjustment of laser parameters (intensity and timing).
- Increase system pulse rate to a maximum of 320MHz
- Provision on-board average photon number sensing
- Provision of a pulsed mode for alignment and data lasers
- Design of a self-contained clock PCB

A schematic of the driver arrangement is shown below.

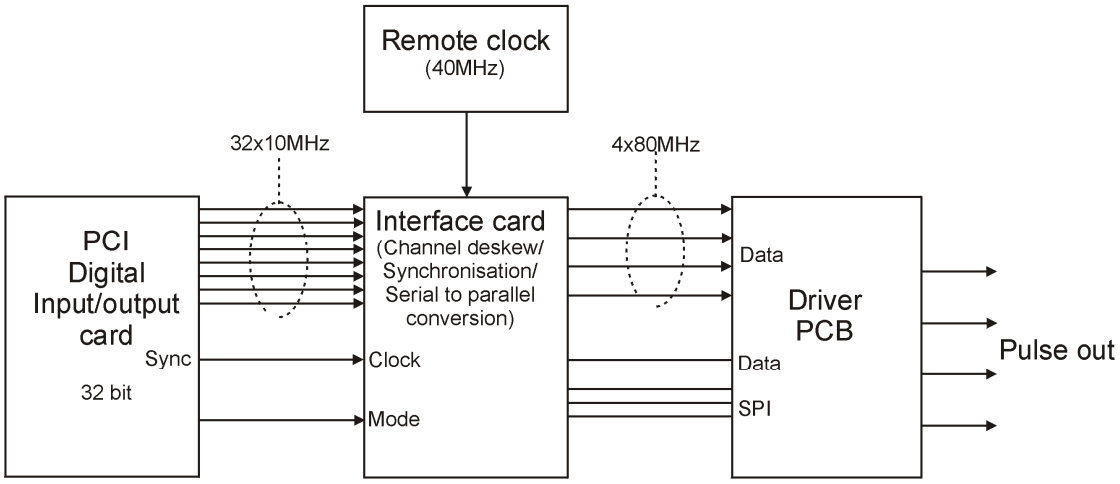


*Figure 7.1. Diagram of the "Mark II" driver. A PCI card feeds 32 data lines to an interface PCB which performs a serial to parallel conversion before feeding the driver PCB located in the Alice optical head.*

The Mark II driver was designed in two parts such that common functions were located on an interface board, whilst particular functions were placed on a driver board. The reason for this was that the quantity of required circuitry was too bulky for the Alice module and also required significantly more power. In addition the interface board was also designed to drive a novel Alice transmitter which, although beyond the scope of this thesis, will be briefly described in the following chapter.

[11] Whilst the author was responsible for all of the electronic design, build and testing for the work described here, acknowledgment is made for the help of my colleague, James Cooper, for digitising the designs and pointing out my mistakes.

### *7.2.1 Interface PCB*

As a compromise (to a complete redesign) it was proposed to use the spare bandwidth available on the Digital Input/Output (DIO) card. The NudaQ PCI 7300 DIO card (as described in the previous chapter) possesses 32 input/output lines which are available for data transfer. These lines can send or receive data at speeds up to 20MHz although the card is most stable at a transfer speed of 10MHz. The combination yields a 32 bit word running at 10 MHz. By using a synchronous 8-bit serial to parallel conversion, a 32 bit, 10MHz word could be converted to a four bit word running at 80MHz giving a significant gain in transmission speed. In addition to bit rate increases the opportunity was taken to improve general system performance. To this end, a switch in technology was made to Positive emitter-coupled logic (PECL) from TTL based logic. This allowed the use of ECL integrated circuits with much faster transmission rates, better jitter performance and higher noise immunity. A schematic of the interface board is shown below.

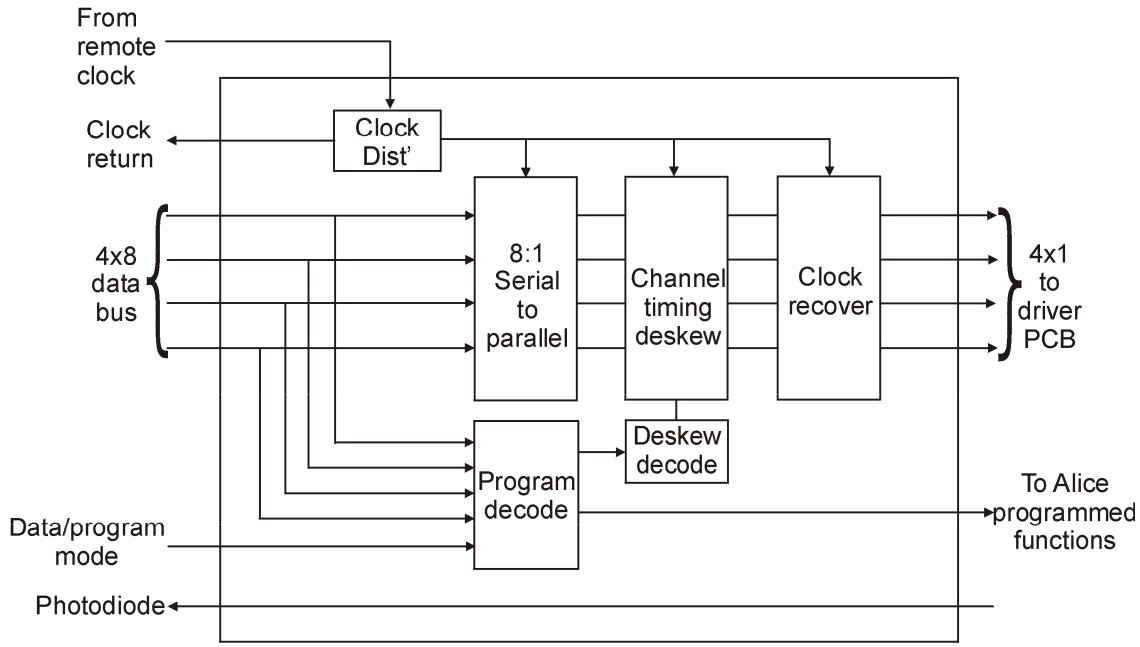


*Figure 7.2. Schematic of the interface board. The board converts a 32 bit parallel data to 4x8 bit serial data. The board also provides access to two modes, programming and data.*

In order to obtain the highest bandwidth possible for data transmission, two modes of operation were introduced:

- Mode 1, programming
- Mode 2, data transmission

These modes are explained in more detail below:

### *7.2.1.1 Programming mode*

This mode of the board was created to allow the setting up of various system parameters prior to, and at regular intervals during, operation. Programming mode allows the following functions to be programmed:

1. Each data channel is equipped with a PECL (PECL- Positive Emitter coupled logic) digital delay circuit providing a programmable delay variation with a resolution of 20ps. The delays are synchronised to each other and can be individually programmed via a 16-bit interface (half of the data transmission mode bandwidth).

2. The remaining 16 bits were given over to programming the Alice driver board via a combination of an industry standard three-wire serial programming interface (SPI) and individual command lines. These functions are dealt with in more detail in the Alice driver section below.

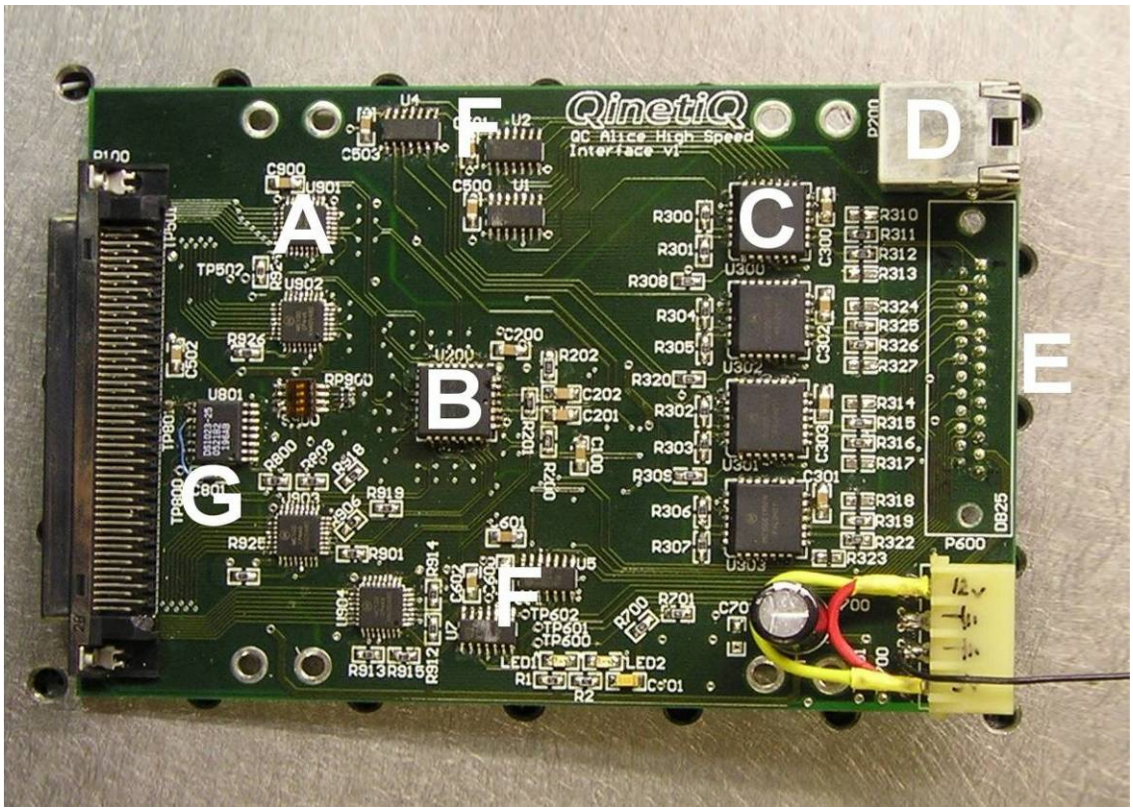


*Figure 7.3. The Interface PCB showing: A. PISO stage, B. Programmable delay, C. Clock recovery, D. Clock input, E. Output, F. Mode switches and G. Delay for DIO clock return.*

### *7.2.1.2 Data mode*

With the system set up, a synchronous data mode was implemented whereby the 32 data lines were split into four buses of 8 lines each. These were each terminated at a PECL serial to parallel converter (SIPO) which synchronously converts each 8-bit parallel input word to a single 8-bit serial output word.

The resulting four serial data channels were then fed through a programmable delay (described above) to a clock recovery circuit (a PECL NAND gate combining a clock pulse with a voltage level to give a pulse train). The serial data was then transmitted over miniature co-axial cable to the Alice driver board.

Synchronisation for all modes was provided from the newly designed remote clock PCB described below. The clock was fed through a PECL clock buffer IC providing eight clock outputs for distribution around the board and back to the DIO card (via a further delay). The circuitry was realised on a good quality PCB with dimensions consistent with an IDE 3.5" hard disk drive (HDD) footprint. A photograph of the finished board is shown in Figure 7.3 above.

### *7.2.2 Alice driver PCB*

The Alice driver PCB was designed to implement the signals delivered from the interface board described above. Signals arriving from the interface card were appropriately terminated and then, depending on function, passed to the next stage. A schematic of the PCB is shown below.

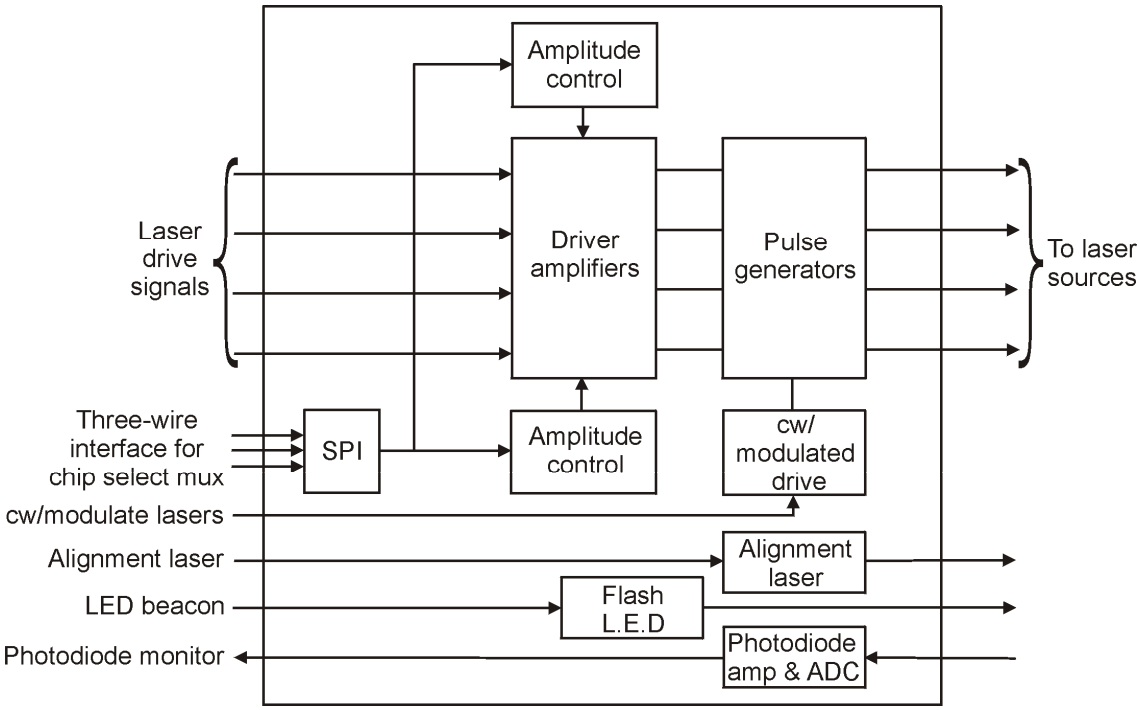


*Figure 7.4. Schematic of the Alice driver PCB.*

The PCB was powered by a DC-DC converter supplying +/-5V at +/-500mA and fed from several commoned conductor wires at 5V. A photograph of the Alice driver PCB can be seen below in Figure 7.5.

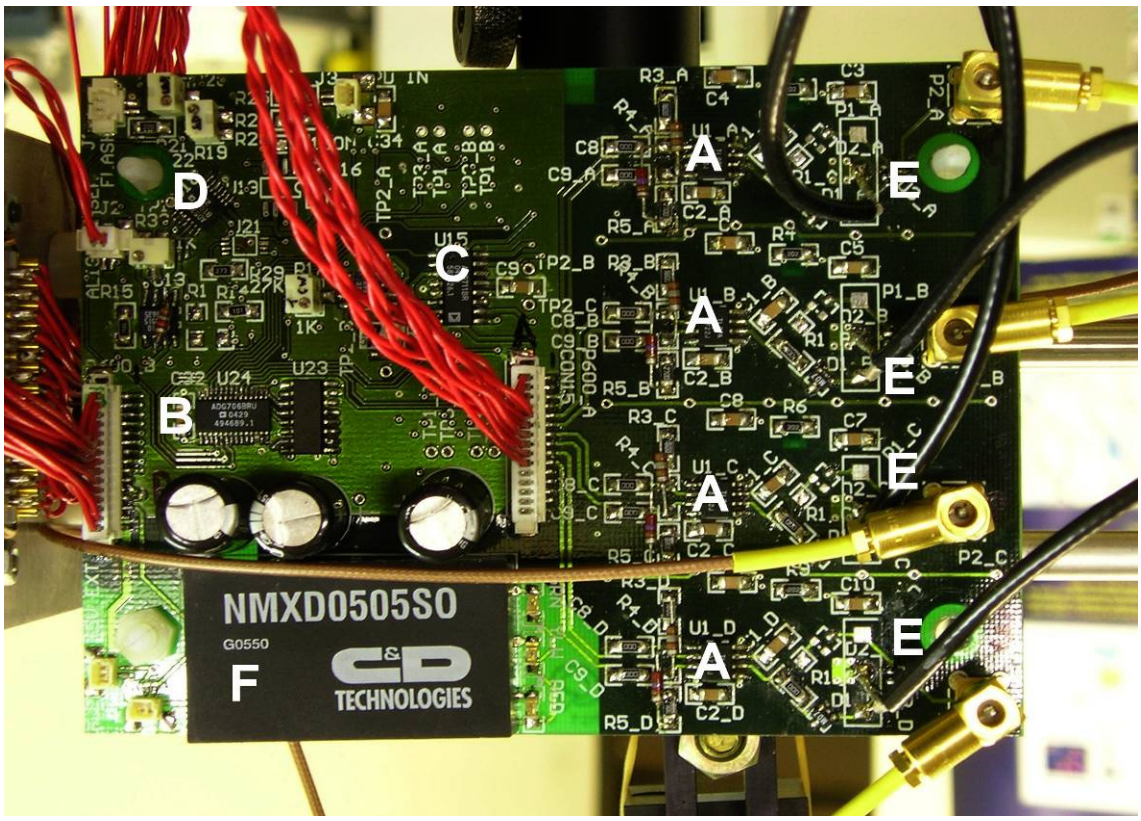


*Figure 7.5. Photograph of the Alice driver PCB showing A. Driver amps, B. Multiplexer, C. C.W. analogue switches, D. Photodiode ADC, E. Delay lines and output & F. DC-DC converter.*

#### *7.2.2.1 Programming*

Programming signals were delivered in two ways. Firstly, a three wire programming interface with a multiplexer was implemented to allow up to 16 ICs to be individually programmed. The following programmable functions were provided by ICs containing a non-volatile memory:

- Data laser intensity control (×8)
- Average photon number sensor:
  - DAC (reverse bias voltage for photodiode)
  - ADC (output digitisation)
  - Photodiode gain control
- Alignment laser intensity

The second mode of programming was by direct control. This method was used for the following functions allowing them to be switched individually from the DIO card in the controlling PC.

- Alignment laser On/Off/pulsed
- C.W. channels On/Off/Pulsed
- LED beacon On/Off

#### *7.2.2.2 Operation*

Operation of the QKD system was much the same as the Mark I system. The main difference was the inclusion of the intensity control of the data lasers. The laser output intensity was monitored by a PIN photodiode placed in the Alice optical head. The photodiode was connected in photovoltaic mode with a programmable DAC controlling the reverse bias voltage (and thus the sensitivity and bandwidth). The output of the diode was then amplified by a transimpedance amplifier ($\times 10^8$) and then a further programmable gain stage. Finally the amplified photodiode output was sampled with an ADC with the output being fed back to the DIO card and used to set the intensity of the lasers.

The lasers were driven by high speed data signals delivered by co-axial cable. The signals were transmitted using PECL voltage levels and terminated with a combination of suitable resistors giving a termination impedance of approximately 50Ω at an average voltage, of approximately 3.3V (PECL standard). The differential signals were then fed directly to the input of the laser drive amplifiers. The amplifier used was, as in the Mark I system, the proven OPA699 voltage limiting amplifier by Texas Instruments.

Intensity adjustment was achieved by using programmable potential divider circuits to place a limiting potential on the OPA699 pins 5 & 8 which are provided for that purpose. The driver amplifier output was then limited to a preset positive and negative voltage which had the effect of limiting the amount of charge placed into the pulse forming network (PFN). This had the further effect of limiting the amount of charge dumped into the load (Laser diode) after cut-off of the step recovery diode contained within the PFN. A set of typical output pulses of the system is shown below in Figure 7.6 below. As before the pulses are clean and symmetrical and have a small afterpulse. Like before, this is probably caused by an impedance mismatch between the driver circuit and laser diode or possibly even the measurement apparatus.

For the slower signals, a TTL voltage level was used which, after transmission via co-axial cable, was terminated with a 150Ω resistor and regenerated using an appropriate logic gate.

Finally, as an experiment, analogue switches were added to the alignment laser and c.w. data laser circuitry. This was included in the circuit to test the viability of implementing an optical classical channel using existing devices embedded in the optical head (such as the alignment laser).

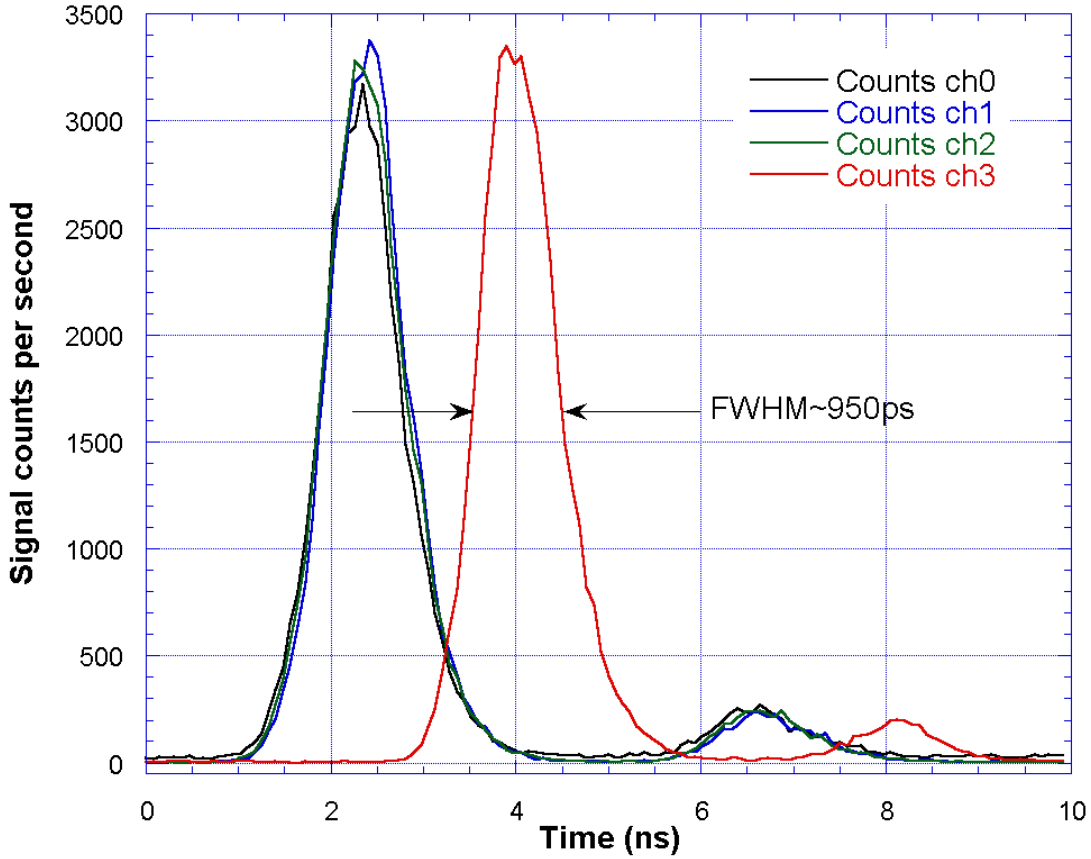


*Figure 7.6. Mark II PCB optical output pulses from the four channels at 80MHz. Pulses are uniform with a full width half maximum of approximately 950ps.*

### *7.2.3 Remote clock*

The idea behind a remote clock board was to provide a versatile and accurate clock for use in any of the QKD systems without tying expensive crystal oscillators to any one system. To this end a PCB was designed to hold an oscillator and all the electronics necessary to supply:

- 10MHz sine wave, 1V peak-peak (raw OXCO output)
- 10MHz squarewave, delayed, inverted and buffered outputs
- Programmable 20/40/80/160MHz multipliers
- ECL/LVDS/CMOS/TTL outputs as required

The circuitry was realised on a commercial quality PCB with dimensions consistent with an IDE 3.5” hard disk drive (HDD) footprint. Power was supplied by a Molex-type HDD power connector. A photograph of the finished PCB is shown below.

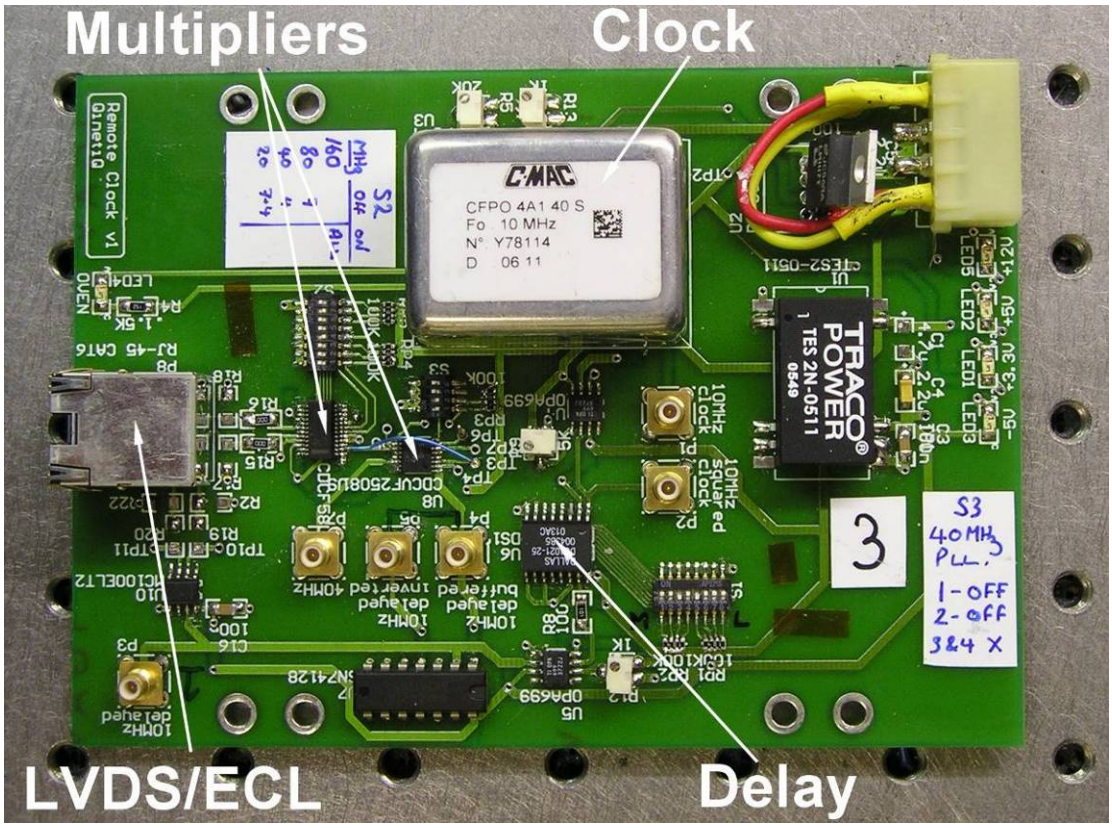


*Figure 7.7. The remote clock PCB. Fitting into a standard 3.5" HDD bay the card provided multiple frequencies in multiple formats including ECL and low voltage differential signalling (LVDS).*

The clock was based on the previous clock circuitry described in chapter 6. The inclusion of the multiplier stages, both incorporating internal phase-locked loops contributed very little in the way of jitter. The use of high quality I.Cs and construction techniques allowed the clocks to retain their excellent performance.

## 7.3 Daylight operation[12]

In order to be efficient and cost effective free-space optical links are required to operate continuously. For systems operating at high latitudes (such as North America or Northern Europe) during the summer months or at high altitudes (including space), where a system may spend close to 100% of its working time in daylight this means a system must possess the ability to operate in daylight. In conventional free-space optical systems this is not a problem as increased noise due to solar background can be offset by increasing the signal power. By contrast, QKD systems, operating at extremely low signal to noise ratios, do not have this luxury. The security of the system depends strongly on the average photon number, $\mu$, which is tightly bounded by theoretical security proofs with the result that even for Decoy State systems the power per pulse of the transmitted beam is still of the order of a single photon. This restriction can lead to high signal losses due to atmospheric effects (as we have seen in previous chapters).

Also related to the low signal to noise ratio of a QKD system is the high background count associated with daylight. The background count in a single photon detector contributes directly to the error rate of a QKD system. If the error rate is too high the system is unable to efficiently distil a usable secure key. In addition, if the background is excessive, the detector can saturate, cease to function correctly or even be destroyed.

For these reasons, the daylight operation studies commenced with gaining an understanding of the background radiation experienced by a QKD system and ways of reducing it. Work then continued with modelling of the atmospheric environment with respect to solar background and absorption spectra. Possible wavelengths of operation and suitable sources for use at this wavelength were then evaluated.

Finally, several methods of reducing background radiation were investigated experimentally with the resulting design applied to the compact QKD. An extended trial was then conducted to assess the efficiency of the design.

[12] During this piece of teamwork the author was responsible for background measurement and all of the work pertaining to the selection of suitable sources for QKD. The MODTRAN modelling used throughout this chapter was provided by my colleague, Dr. David Taylor.

### *7.3.1 Background measurement*

Measurement of the system background was recorded over several days using the apparatus shown in Figure 7.8.

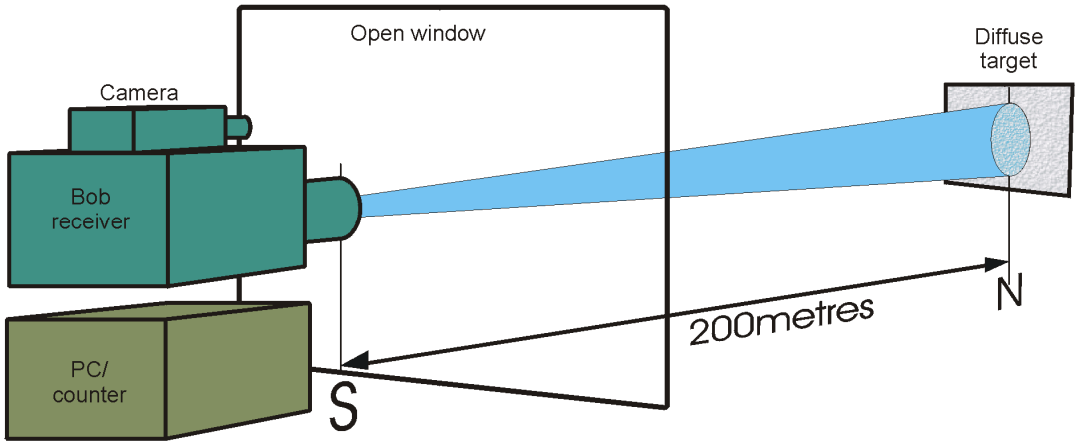


*Figure 7.8. Equipment set-up for background measurement. Bob "looks" at a South facing diffuse reflector and the average count rate is recorded over several days.*

A Bob receiver was positioned at a suitable window facing approximately North and fitted with "standard" optics consisting of a lens (f=125mm, d=50mm) and a filter centred at wavelength 670nm with full width half maximum bandwidth of 10nm. The field of view of the detector was made to be incident upon a polystyrene covered plywood board approximately $1m^2$ at a range of 200m. A software programme was then written to record the background count level originating from the polystyrene target every minute over several days thus allowing the variations in weather conditions and their effect on background counts to be monitored. Polystyrene material was used as it displays excellent diffuse scattering characteristics and can be regarded as a near-perfect Lambertian reflector. Neutral density filters (O.D. ~2) were placed in front of the receiver telescope to maintain the linear response of the detector and avoid saturation. The rationale behind this arrangement was that rather than placing Bob facing South, a more representative scenario was to have Bob view a predictable, efficient diffuse reflector which itself was facing South and thus reflecting the integrated solar background at Bob. In addition, to gain a qualitative idea of the variation of the background a camera was set up to view the same scene as the Bob detector and record an image every 15 minutes. The result of the background measurement is shown below in Figure 7.9.

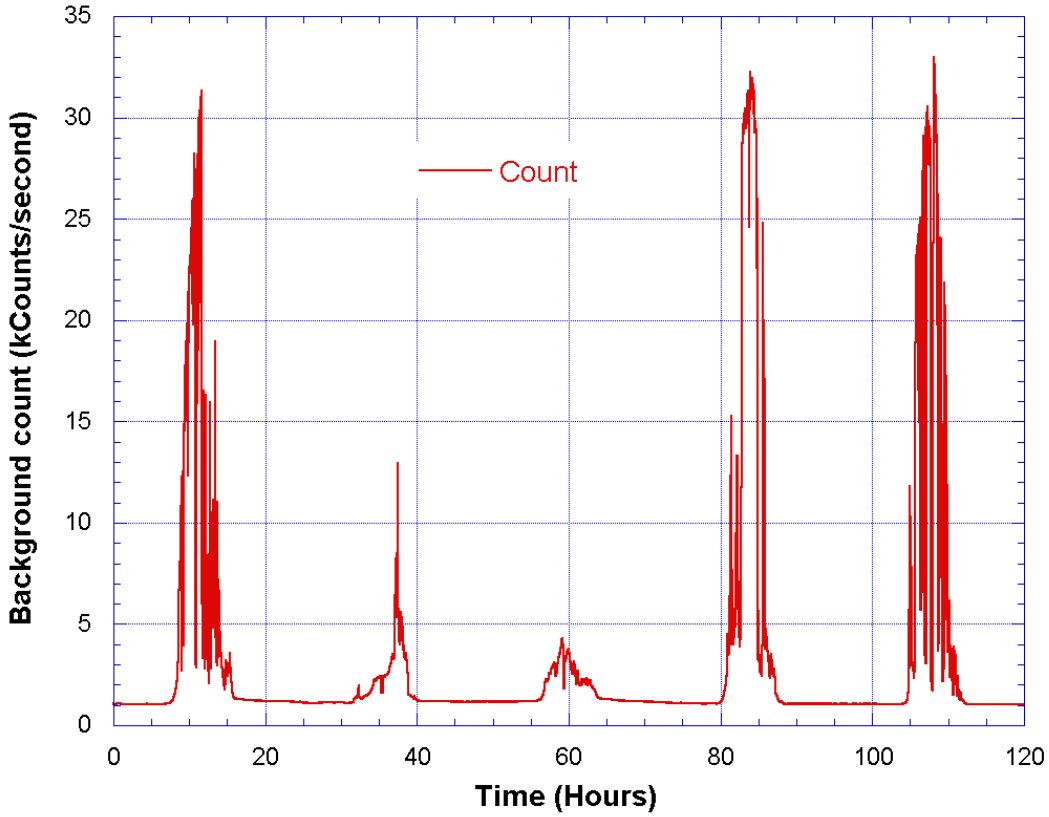


*Figure 7.9. Average background as seen by Bob receiver facing a diffuse reflecting panel facing south.*

Examination of the plot gives an idea of the scale of the problem. At night Bob experiences an average background count of approximately 1kCounts/second per detector (which is approximately the same as the dark count of the detector). From previous experiments it is well known that the QKD system can function at this background level so this provides a convenient benchmark. As the plot moves through the night to the first day, it can be seen that the background rapidly increase to nearly 32kCounts/second. The second and third days appear to have a much lower count rate as a result of the sky being rather overcast. The final two days are again bright with a return to a large background rate of approximately 32kCounts/s. However, when taking into account the Neutral density filters (O.D. =3) at the Bob receiver, the actual count rates are calculated to be in excess of 3Mcounts per second.

This suggests that in order to function efficiently during bright daylight the background must be selectively reduced by three orders of magnitude or 30dB.

By way of further illustration of the problem, the photo below shows the contrast between bright and sunny day and late at night from the point of view of the receiver.

*Figure 7.10. The view from the Bob receiver. The red circles mark the White diffuse reflecting target. Bobs field of view falls within the 1m$^2$ target area. The difference in background is approximately 30dB.*

### *7.3.2 Background modelling*

Most of the daytime background radiation which enters the Bob optical system originates from the Sun. The use of atmospheric modelling software such as MODTRAN allows estimation of the spectral distribution of the solar background. Coupled to the ability to model atmospheric transmission properties, this allows the expected background levels at Bob to be estimated. The plot below shows the modelled solar irradiance estimated over the visible spectrum:

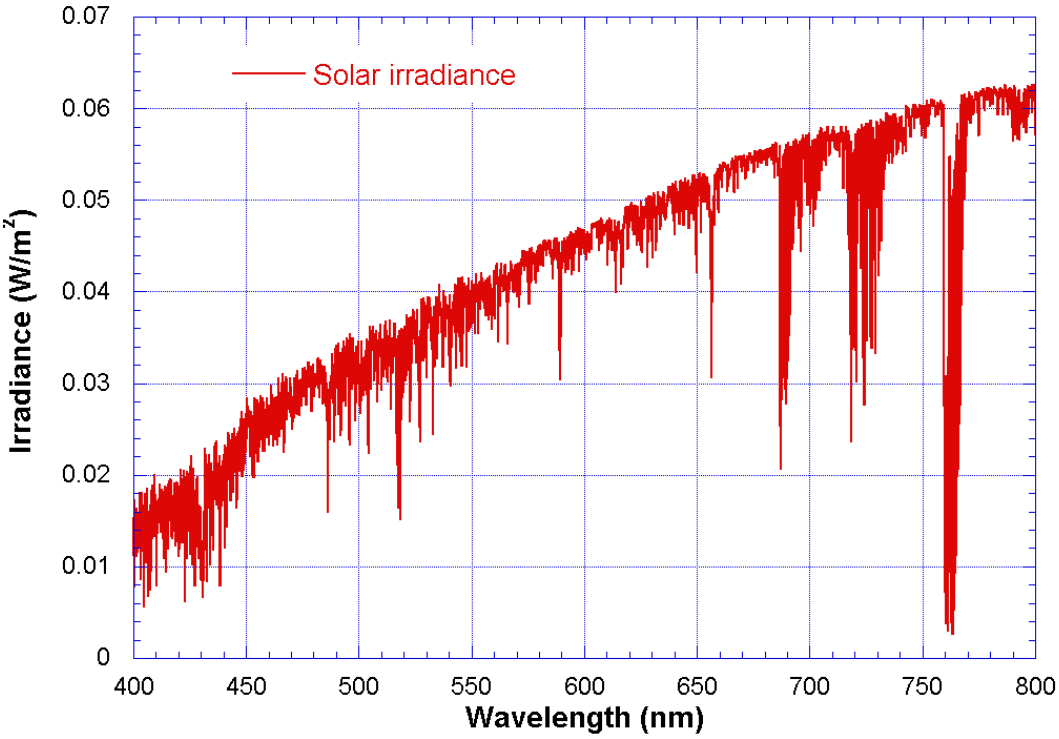


*Figure 7.11. Solar irradiance estimated using MODTRAN software for the visible radiation band, 400-800nm.*

This data allows an estimation of the amount of solar background entering the Bob receiver to be made:

Power entering the Bob aperture:

$$P = L(\lambda)F(\lambda)\pi(r\phi)^2 \frac{\pi d}{4r^2} R \qquad (7.1)$$

Where:

L(λ) is the solar irradiance as a function of wavelength, λ,

F(λ) is the filter transmission function,

r is the range to target,

$\phi$ is the field of view,

$d$ is the collecting lens diameter

and $R$ is the scene reflectivity.

The irradiance level must be corrected for latitude and atmospheric air mass attenuation. Bob optics are as given above.

To calculate the expected count rate $R_{bg}$ we must include other loss factors such as reflections at glass-air interfaces, filter losses and detector efficiency:

$$R_{bg} = \frac{n_{bg} t_l^{n_s} t_f \varepsilon}{n_{\det}} \qquad (7.2)$$

Where:

$n_{bg} = \frac{P}{E(\lambda)}$ is the number of photons per second of energy E,

$t_l$ is the transmission loss at each glass surface $n_s$

$t_f$ is the transmission through the RG650 filter,

$\varepsilon$ is the detector responsivity

and $n_{det}$ is the number of detectors over which the light is distributed (×4).

This calculation gives an estimated background count rate of $4.2\times10^6$ counts per second(cps). Compare this with the measured value of $3.5\times10^6$ cps and one sees good agreement given that the background depends on many factors which change on several different timescales.

#### *7.3.2.1 Background reduction*

Having considered the problem above, clearly, in order to operate the system during daylight a significant reduction in background of the order of 30dB must be accomplished. Furthermore, the reduction must be selective as it would be a pointless task to reduce the transmission of the whole spectrum by 30dB.

In an optical system of this type there are three degrees of freedom which can be used to reduce the background – spectral, spatial and temporal.

In the Spectral domain, the incoming radiation can be filtered effectively using combinations of different types of filter in order to isolate the signal wavelength. In addition, a part of the spectrum with low background can be chosen for operation. Spatially, the field of view can be controlled such that the receiver is gathering light from the smallest area possible. In addition, baffles can be placed so as to trap any off-axis radiation entering the receiver. In the temporal domain, a timing window can be used to restrict the operation of the detectors to times when signal photons are expected and ignore all other detections.

#### *7.3.2.2 Selection of wavelength of operation*

Selection of an operating wavelength can be complicated. It is not necessarily enough just to consider the background. There are additional factors which can have an effect on system performance such as detector responsivity, atmospheric transmission and source availability. It is also worth noting that a low level of background light at a particular wavelength may be due to absorption by atmospheric constituents which will also efficiently absorb the signal. To help make an informed selection, accurately modelled atmospheric properties can be combined with spectral response data of detectors to give an overall idea of how a system might behave.

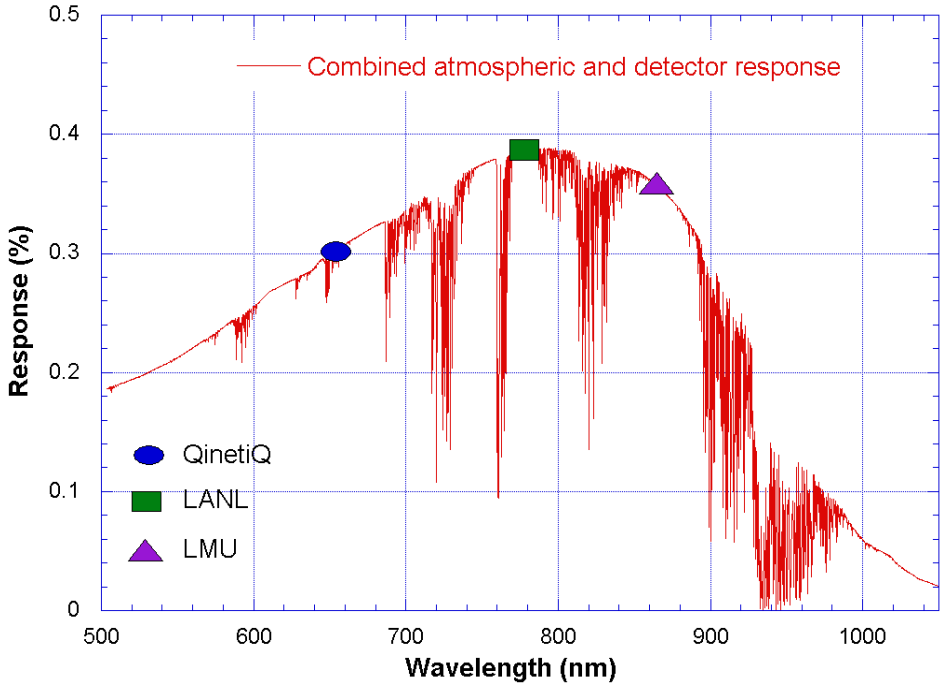


*Figure 7.12. Atmospheric transmission combined with detector response for a Perkin-Elmer Silicon avalanche detector. Coloured shapes represent wavelengths of operation for three free-space QKD systems.*

As an example, the figure above shows a combination of atmospheric transmission as modelled by MODTRAN combined with the response of a Perkin-Elmer C30902 avalanche photodiode. As can be seen from the graph, the efficiency of the detector greatly modifies the atmospheric transmission characteristic with efficiency falling off rapidly at wavelengths greater than 900nm. The wavelength of operation for three free-space systems are shown with QinetiQ [1] (635nm) in blue (circle), Los Alamos national laboratories [2], U.S. (772nm) in green (square) and LMU, Munich [3] (850nm) in purple (triangle). It is clear that these wavelengths have been chosen to coincide with a combination of good detector response and efficient atmospheric transmission.

Whilst it is not always sensible to operate at a wavelength where background radiation is at a minimum, there are some occasions when this is appropriate. If one compares the atmospheric transmission spectrum with the solar irradiance, certain wavelengths can be found which combine high transmission with low background levels. These wavelengths are termed Fraunhofer lines and they owe their existence to absorption of solar radiation in the atmosphere of the sun. Although there are several hundred known Fraunhofer lines, most of them have an extremely narrow width. A few, however, possess sufficient bandwidth to be useful and fall into the part of the spectrum usable by short wavelength QKD systems [4]. These wavelengths are shown below in Table 7.1:

| Wavelength (nm) | Width (nm) | Width (GHz) | Species |
|---|---|---|---|
| 434.0475 | 0.2855 | 454.6 | H |
| 486.1342 | 0.3680 | 467.2 | H |
| 517.2698 | 0.1259 | 141.2 | Mg I |
| 518.3619 | 0.1584 | 176.9 | Mg I |
| 656.2808 | 0.4020 | 280.0 | H |
| 849.8062 | 0.1470 | 61.1 | Ca II |
| 854.2144 | 0.3670 | 150.9 | Ca II |
| 866.2170 | 0.2600 | 104.0 | Ca II |

*Table 7.1. Wavelengths of the useful Fraunhofer lines in the visible solar spectrum [5].*

Of these lines, it would appear most appropriate to attempt to use the so-called Hα line (although, actually several overlapping fine structure lines [6]) situated at 656.28nm.

This is because it has a relatively wide bandwidth and is already situated close to the wavelength of the existing system and thus would require only a change of sources and filters. A plot of the Hα Fraunhofer line is shown below in Figure 7.13. Examination of the plot shows a reduction in background of approximately 7dB over a FWHM of 0.2nm.

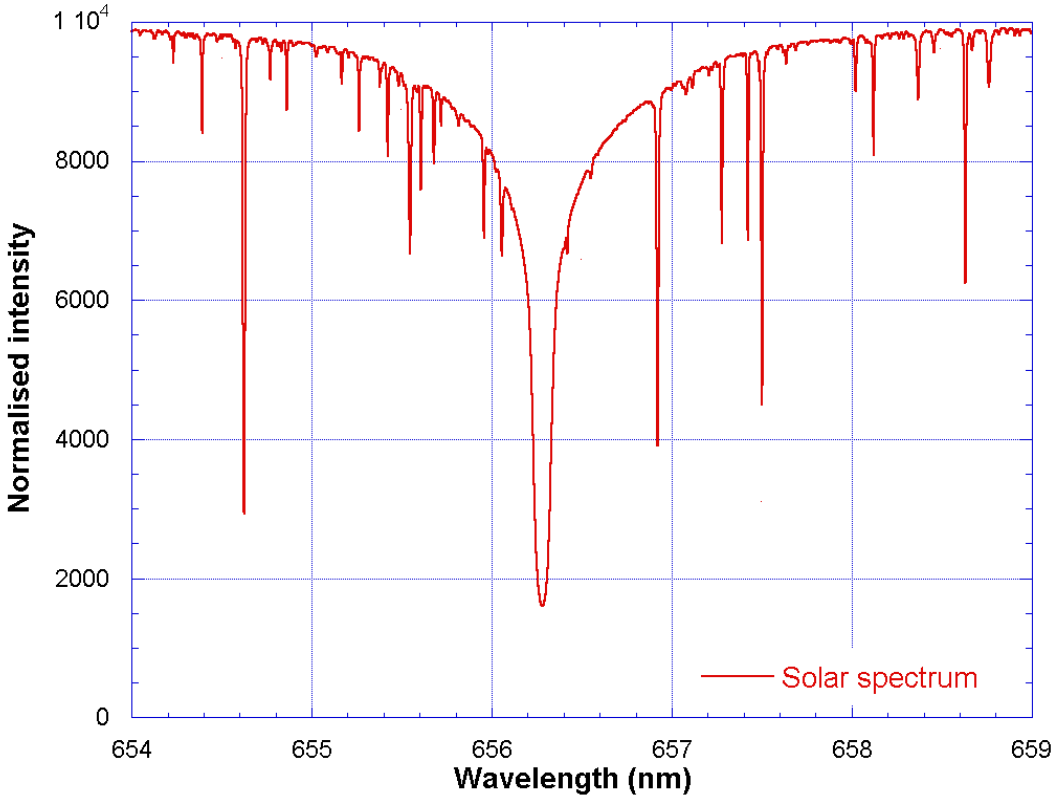


*Figure 7.13. The Fraunhofer Hα line at 656.28nm. The line is approximately 0.2nm wide and at its peak gives a reduction in background of ~7dB (after L. Delbouille, G. Roland & L. Neven (1981): Photometric atlas of the solar spectrum from λ = 300nm to λ = 1000nm, 1981, Data sourced via BASS2000, L'Observatiore de Paris).*

Use of this wavelength could provide a significant advantage for a free-space QKD system, provided the transmitter and receiver could stay locked to this wavelength. Conveniently, this wavelength is very popular with solar astronomers and a wide variety of off-the-shelf filtration optics are available.

### *7.3.3 Comparison of optical sources for QKD*

Light emitted from laser devices typically arises due to a well-defined atomic transition. In the case of semiconductor lasers, the wavelength is defined by the so-called energy bandgap of the semiconductor material used to fabricate the laser. An additional constraint on the wavelength of the output radiation is set by the dimensions of the device itself. In the case of the semiconductor laser, the device is typically several tens of microns long and this length gives rise to a set of "cavity modes" which can propagate within the laser gain bandwidth. This phenomenon can be seen in the spectrum of an edge emitting laser diode below in Figure 7.14.

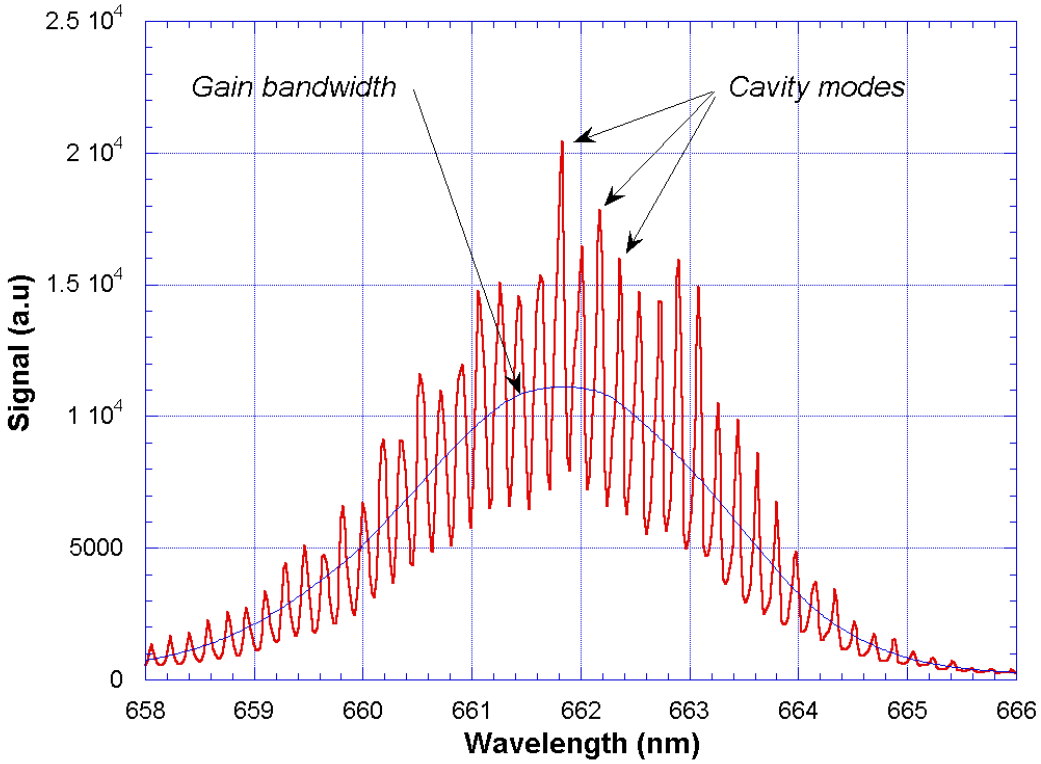


*Figure 7.14. Low and high resolution spectrum of a laser diode showing gain bandwidth and cavity modes.*

The smooth curve, measured with a low resolution monochromator grating (150lines/mm) shows the effective gain spectrum of the material itself.

Meanwhile, use of a high resolution grating (1200lines/mm) reveals a periodic structure superimposed on the gain curve of the material which is characteristic of a set of cavity modes.

Another property of laser diodes is that of temperature dependence of the spectral emission characteristic. All semiconductors exhibit some form of temperature dependence in spectral output, the magnitude of which depends on the type of material used in the fabrication process.

The majority of semiconductor lasers available commercially and used in the QinetiQ QKD system are GaAs edge emitting devices and can shift in wavelength, in this case, by as much as 0.17nm/$^{o}$C. The effect can be seen below in Figure 7.15.

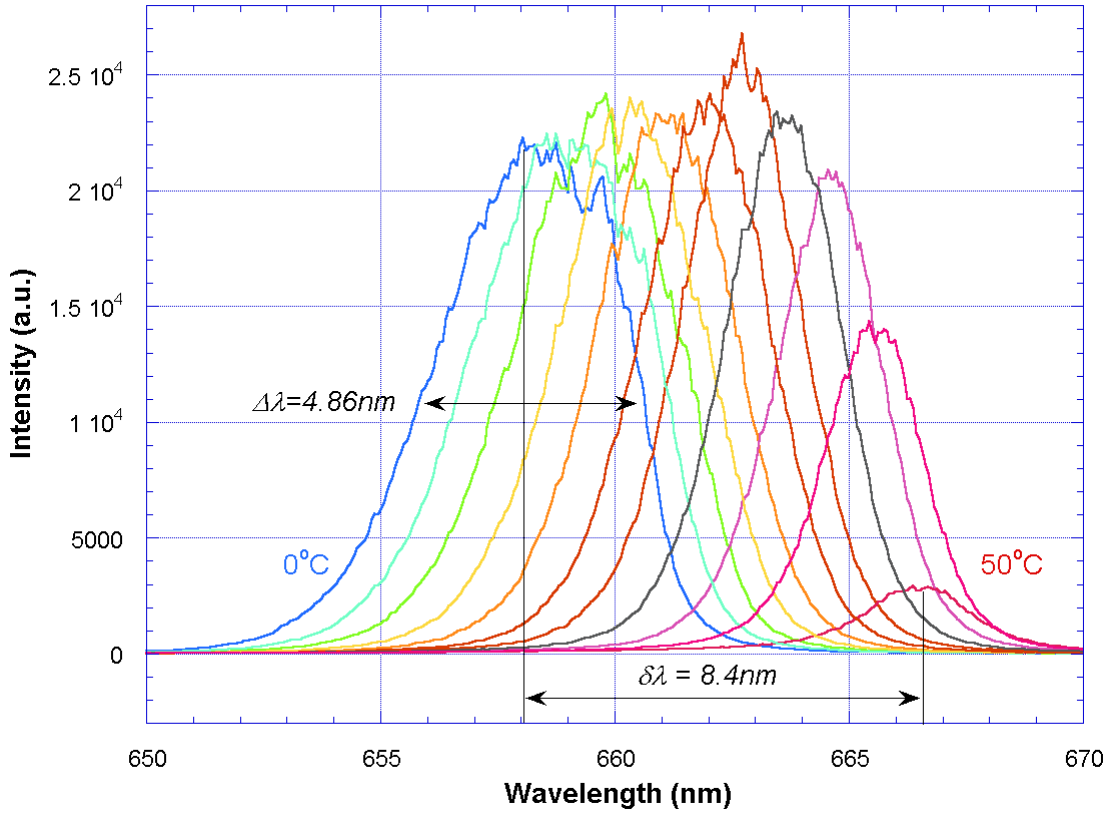


*Figure 7.15. Plot of spectral output of a laser diode heated to 50$^{o}$C then cooled in 5$^{o}$C stages to 0$^{o}$C. Laser spectral bandwidth narrows whilst the whole spectrum moves to longer wavelengths as the temperature increases.*

Here a laser diode has been heated to 50$^{o}$C and then cooled in stages to 0$^{o}$C. At each 5$^{o}$ stage the spectrum was measured and then plotted yielding the graph shown. The heating mechanism used in this case was a combination of ohmic heating and ambient temperature change.

Examination of the graph shows that the laser bandwidth at 0$^{o}$C is approximately 4.8nm dropping to approximately 2.5nm at 50$^{o}$C, which is fairly typical behaviour for this technology. However, if one now looks at the gross variation in output wavelength, $\delta\lambda$, it can be seen that this is approximately 8.4nm, over twice the bandwidth of the laser (and nearly three times that at 50$^{o}$C). Furthermore, it may be seen that at the highest temperatures, the laser intensity is much reduced. This can be due to a number of intrinsic material effects within the device (i.e. loss of carriers at high temperatures) leading to a larger operating current required to reach threshold (and any given optical output power).

In both cases shown above, tight spectral filtering of the laser output will lead to large variations in intensity of radiation passing through the optical filter at both the transmitter and the receiver particularly as the interference filters are only subject to ambient temperature changes and the filters transmission typically shows a weak dependence on temperature (of the order of ~0.01nm/$^{o}$C). Couple this with the requirement for a very narrow band optical filter at Bob and the situation becomes even worse.

The problem can be seen more clearly below in Figure 7.16. The graph shows the normalised spectra of a single laser diode at temperatures ranging from 0$^{o}$C to 30$^{o}$C. Superimposed over these is the transfer function of a typical narrow band filter with a fairly wide passband of ~2nm.

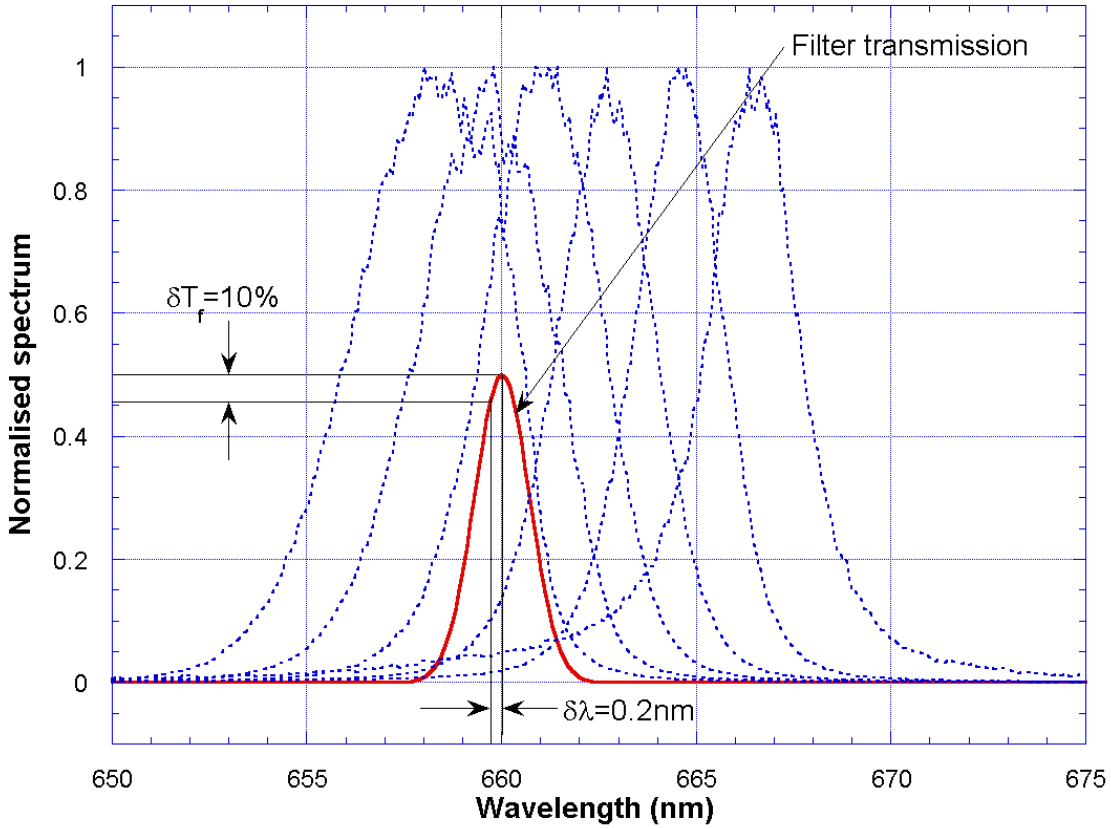


*Figure 7.16. Laser diode spectra with respect to temperature (showing typical narrowband filter function).*

One can see that a temperature change of 30$^{o}$ Celsius moves the spectrum of the source outside the transmission of the filter which would result in complete signal loss.

Furthermore, to maintain a steady output intensity, even to within 10% variation, would require control of the wavelength to within 0.2nm and therefore temperature control to approximately 1$^{o}$ Celsius at both Alice and Bob.

Given that temperature control is costly in terms of components, space, power and engineering, an alternative method of maintaining a steady, monochromatic output would be greatly beneficial.

One method proposed was to use broadband emitters and place them behind a narrowband filter. The output wavelength would then be defined by the filter transfer function rather than the materials from which the source device is manufactured. It was therefore decided to explore other types of source with the intent of identifying characteristics suitable for using in this way. The devices considered with known broadband emission were light emitting diodes (LEDs) and resonant cavity LEDs (RCLEDs). Several devices of each type were procured for testing and comparison with each other to assess their suitability for use as QKD sources.

LED devices are made from the same sort of materials as laser diodes but have no resonant cavity. Moreover, the radiation emitted by LEDs shows none of the characteristics of laser radiation (coherence, monochromaticity, directionality etc.) so, whilst the spectral dependence on temperature is still present it is mitigated by the very broadband emission from these devices.

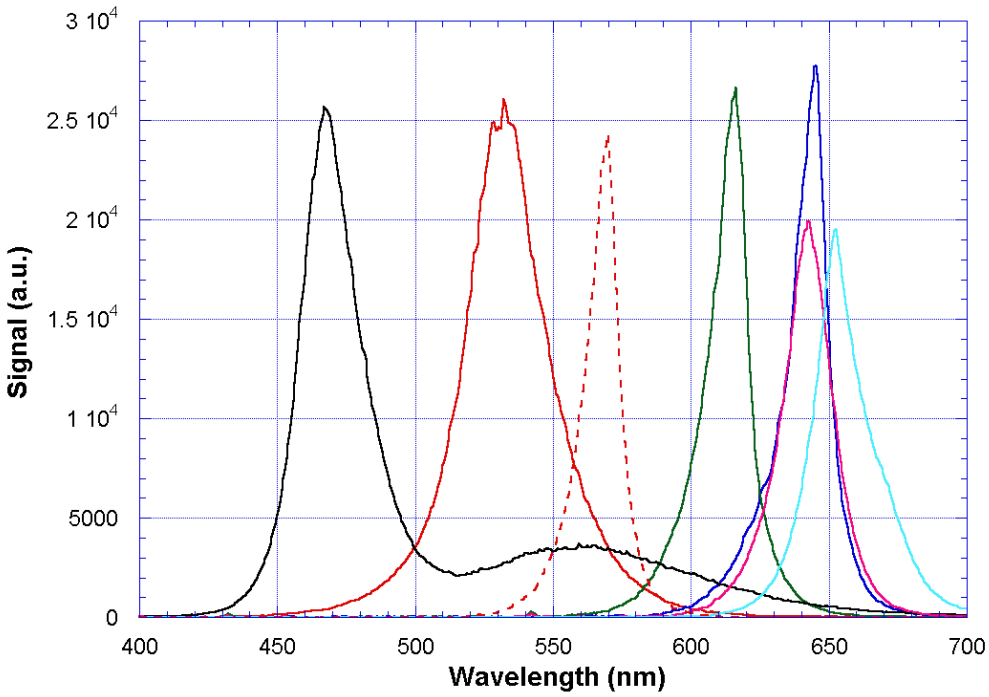


*Figure 7.17. Output spectra of various LEDs. Bandwidths range from 15nm to 50nm FWHM.*

A set of LED output spectra are shown above. These devices were randomly selected from in-house legacy components and serve to show the wavelength bandwidth and diversity of these devices. The narrowest emission bandwidth seen here is 15nm at full width half maximum (FWHM).

Generally speaking, LEDs are not intrinsically fast devices, attainable modulation rates are limited due to their structure (specifically, the junction capacitance) of the device. Typical modulation rates lie in the region of a few tens of Megahertz with pulse widths of microseconds or, at best, a few tens of nanoseconds. A comparison of edge emitting Laser diode (LD) and LED pulses are shown below in Figure 7.18.

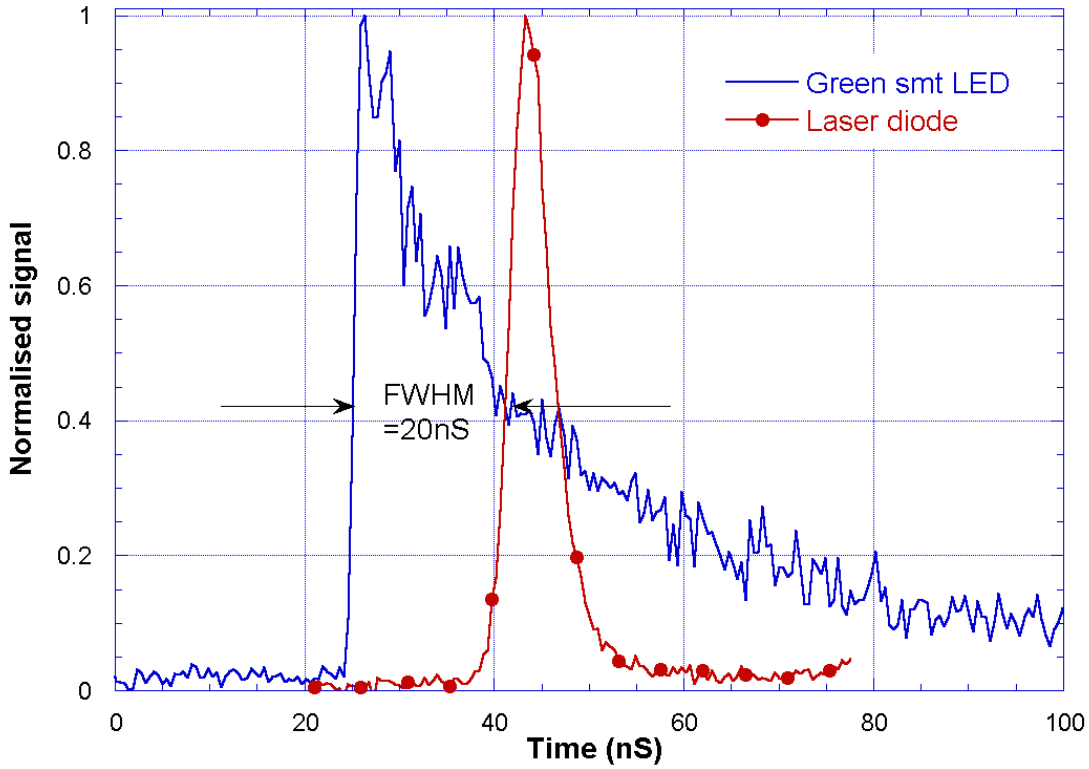


*Figure 7.18. Comparison of LD and LED pulses, both driven from a 1ns electrical pulse. LED pulsewidth is approximately 15ns versus ~5ns for the laser.*

Whilst the LD gives a very fast clean pulse, the LED has a fast risetime but a long tail lasting many tens of nanoseconds. The pulse characteristics of LEDs are therefore generally unsuitable for QKD.

A compromise to these drawbacks may lie in the use of a Resonant Cavity LED or RCLED. These devices are fabricated from the same materials as laser diodes and LEDs but the active area is contained within a Fabry-Perot optical cavity. The resultant structure yields a device with a broader output spectrum than a laser diode but brighter and more directional output than an LED (an extensive review of RCLEDs is given in [7] and [8].

The output spectrum of a legacy RCLED device from previous research is shown below in Figure 7.19 and appears to contain no cavity modes (the short cavity allows only one mode to propagate within the gain bandwidth of the material).

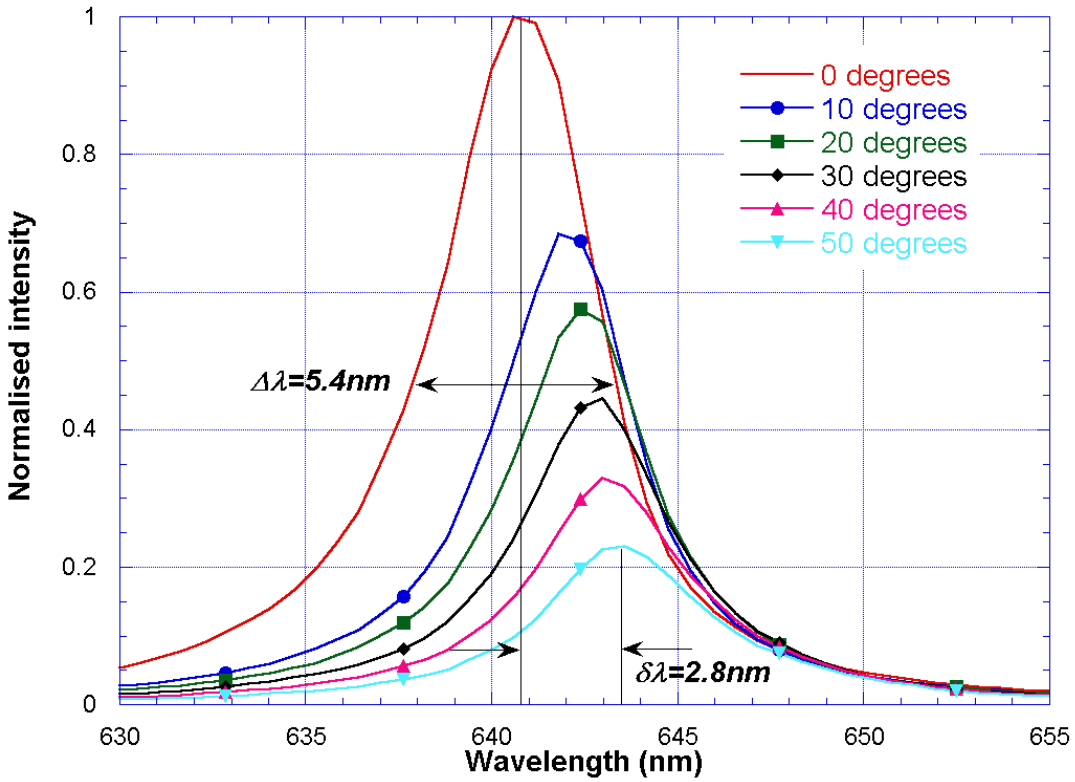


*Figure 7.19. Plot of spectral shift of an RCLED for a temperature variation of 50°C in increments of 10°C. The peak wavelength shifts but stays inside the original spectral feature.*

As the temperature increases the peak output appears to shift to longer wavelengths whilst reducing in intensity.

This is due to the material emission spectrum moving to longer wavelengths and becoming detuned from the resonant mode supported by the cavity within the devices. This behaviour has implications for use of these devices with QKD systems.

As a result of the novel structure employed in the construction of RCLEDs it is possible to obtain pulse widths down to a nanosecond when driven with appropriate electronic circuitry. Figure 7.20 below shows the temporal output from the same legacy RCLED device when driven from a nanosecond electrical pulse. The pulse is clean and symmetrical, with no afterpulsing. The pulse width of 900ps is eminently suitable for QKD applications.

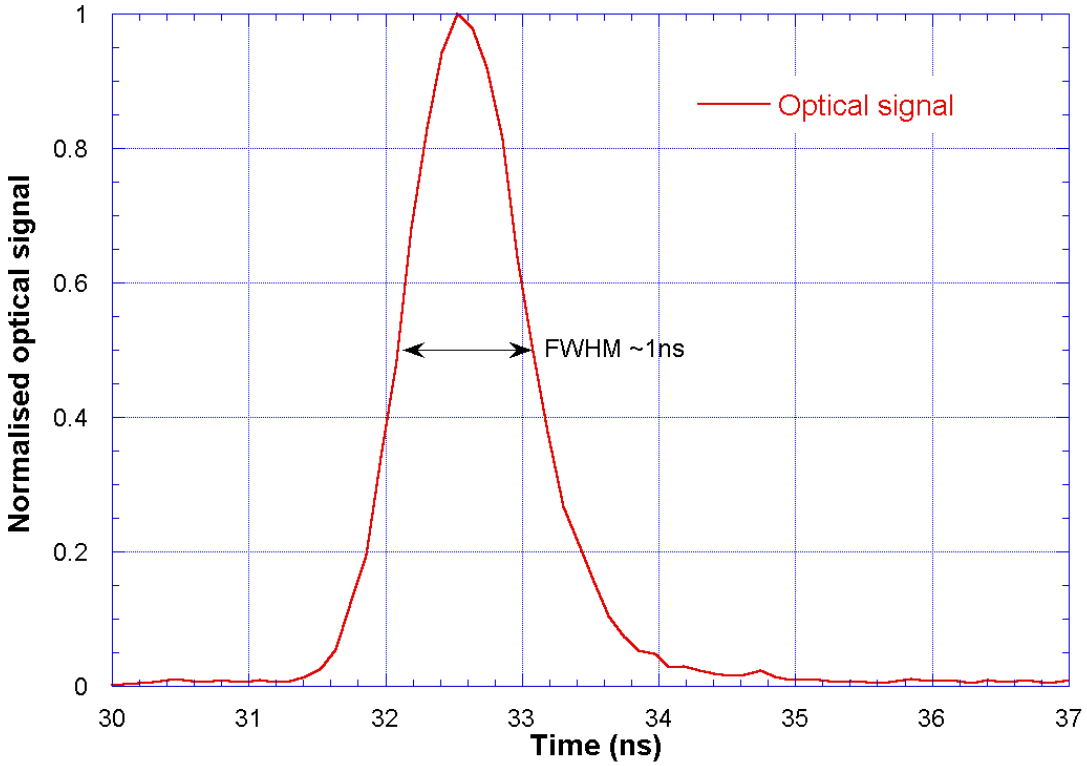


*Figure 7.20. Optical output pulse from a RCLED driven by a nanosecond electrical pulse.*

In summary, all three source types have at least one desirable property from the point of view of simple, compact QKD but also show some disadvantages. The table below summarises the main requirements and characteristics of the tested sources.

| Device type | Pulse width | Temperature stability | Beam quality | Bandwidth | Suitability for QKD |
|---|---|---|---|---|---|
| Laser diode | <1ns | Mediocre | Good | Narrow | High |
| LED | 1ns><1μs | Mediocre | Bad | Wide | Medium |
| Resonant cavity LED | <1ns | Good | Medium | Medium | High |

*Table 7.2. Summary of properties for QKD sources.*

Edge emitting laser diodes (LDs) make good sources for use in QKD systems. They show a sharply defined output spectrum and can produce ultra-short pulses (~100ps). However, they suffer from some significant drawbacks when the system operation is extended to daylight operation:-

- Laser diodes exhibit cavity modes due to their structure. This leads to a periodic gain (and therefore intensity) fluctuation superimposed on the material gain bandwidth.
- Laser diodes can exhibit a strong spectral dependence on temperature. This manifests itself as a spectral drift as the temperature of the device and its surroundings change.

Both of these features would lead to significant output intensity fluctuations from an Alice transmitter unless some temperature controlling hardware was installed into the transmitter module.

Light emitting diodes (LEDs) are candidates for use in QKD systems. They are available commercially in a wide range of output wavelengths and show broadband emission without the cavity modes imposed by an optical cavity. They do, however, suffer from two major drawbacks:-

- LEDs emit into a much larger cone than LDs (an LED may emit over several steradians). This makes it difficult to collect the radiation and focus it through the system optics.
- LEDs do not, as a rule, respond quickly to an electrical input. This can be due to a number of factors related to their construction.

It may be possible to drive these devices correctly or to obtain LEDs that can be driven with ultra-fast pulses but these devices do not appear to be available commercially at the time of writing.

Resonant cavity LEDs appear to show significant advantages over the use of either laser diodes or LEDs in a quantum cryptography system. Their characteristics show several advantages over the use of either LDs or LEDs.

- RCLED emission spectra show less temperature dependence than laser diodes whilst their spectral bandwidth is broader.
- RCLEDs possess no cavity modes, or rather the resonant cavity is so short that only one mode is resonant within the gain bandwidth of the material.
- Due to the inclusion of the optical cavity, these devices can emit directional radiation, making it easy to collect and focus the radiation into a bright spot.

These advantages would appear to make the RCLED a reasonable choice for use in a QKD system. In addition the first telecom window in plastic optical fibre (POF) coincides with the solar radiation minimum situated at the H$\alpha$ absorption wavelength meaning that these devices are also available commercially at the wavelength of choice for daylight operation of QKD.

### *7.3.3.1 RCLED assessment*

With the above results in mind a set of 20 RCLED devices were procured for use in converting the compact QKD system to daylight operation. The devices took the form of a plastic packaged fibre-optic transmitter unit suitable for use in short-haul communication systems with plastic optical fibre (POF) cable [8]. The typical output wavelength of the devices was given as 650nm with a bandwidth 20nm full width half maximum (FWHM). Transmission rates were given as 250Mbps with optical rise and fall times of 2ns each.

The RCLEDS were tested by connecting them to a pulsed electrical source designed to mimic the output pulses of the Alice transmitter. The optical output was then fed via a light guide to a spectrometer with a cooled sensor array, allowing the acquisition of complete spectra. The spectra from the 20 RCLEDs are shown below:-

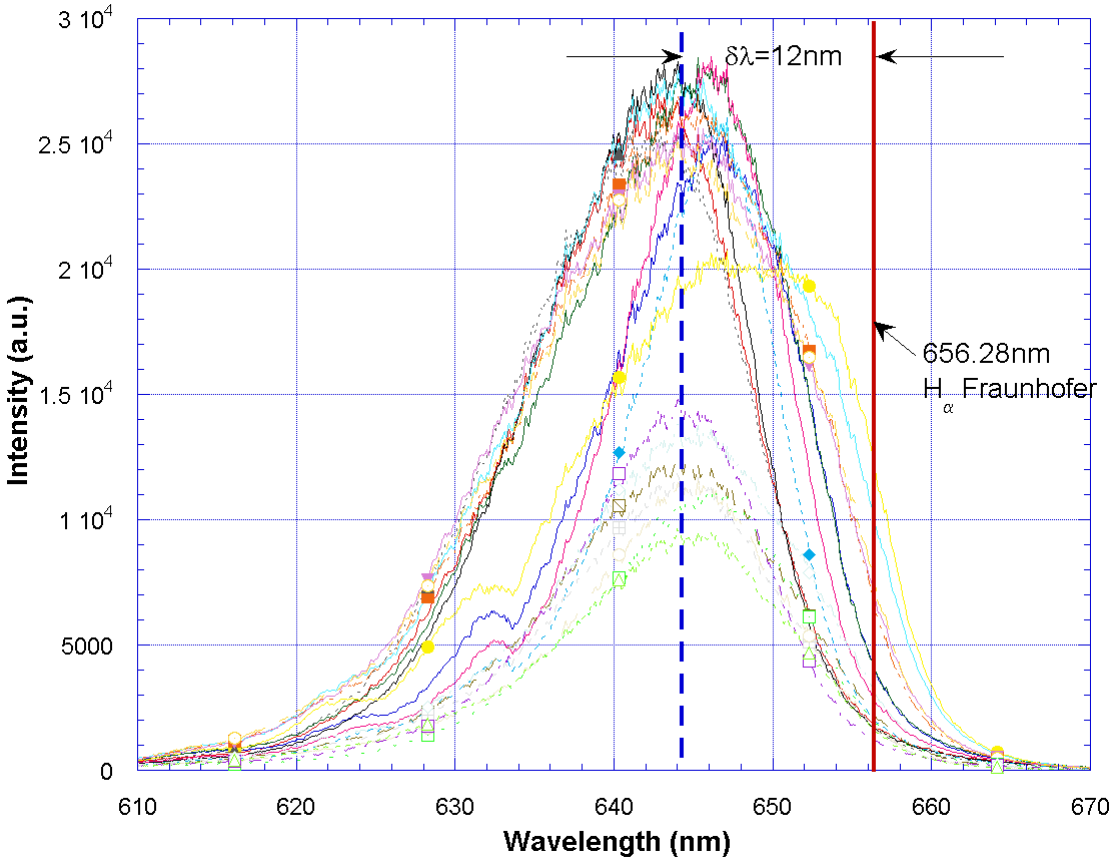


*Figure 7.21. Spectra of 20 RCLEDs. There is a wide variation in output and peak wavelength. All have one thing in common – significant wavelength deviation from the desired wavelength.*

The graph above shows the measured spectra for all 20 of the sources procured for the investigation. Whilst the graph may look somewhat crowded, the point to note is that all 20 spectra are peaked around 644nm on the x-axis (vertical blue dotted line).

This shows that the RCLED devices are well matched with each other, and also that the peak wavelength for the devices tested is somewhat shorter than the “typical peak wavelength” figure quoted on the datasheet.

For comparison, a red line has been drawn where the transmission of an Hα narrow band filter is at its maximum. As can be seen, there is a significant wavelength difference (~12nm) between the two.

The RCLEDs were designed to operate in short haul (<50m) plastic optical fibre (POF) communications applications. The device datasheet [9] quotes a typical data rate of 250Mbps with a rise and fall time of 2ns each. This figure implies that the devices may not have a bandwidth wide enough to operate in the Compact QKD system as the system operates at a data rate of 20Mbps with pulses of 1ns width (FWHM). A pulse of this width requires an electrical bandwidth of a minimum of 1GHz in order to function correctly. The RCLED optical output was collected and analysed using a Perkin-Elmer single photon detector connected to a Hewlett-Packard 53310A Modulation Domain Analyser. The result may be seen below:-

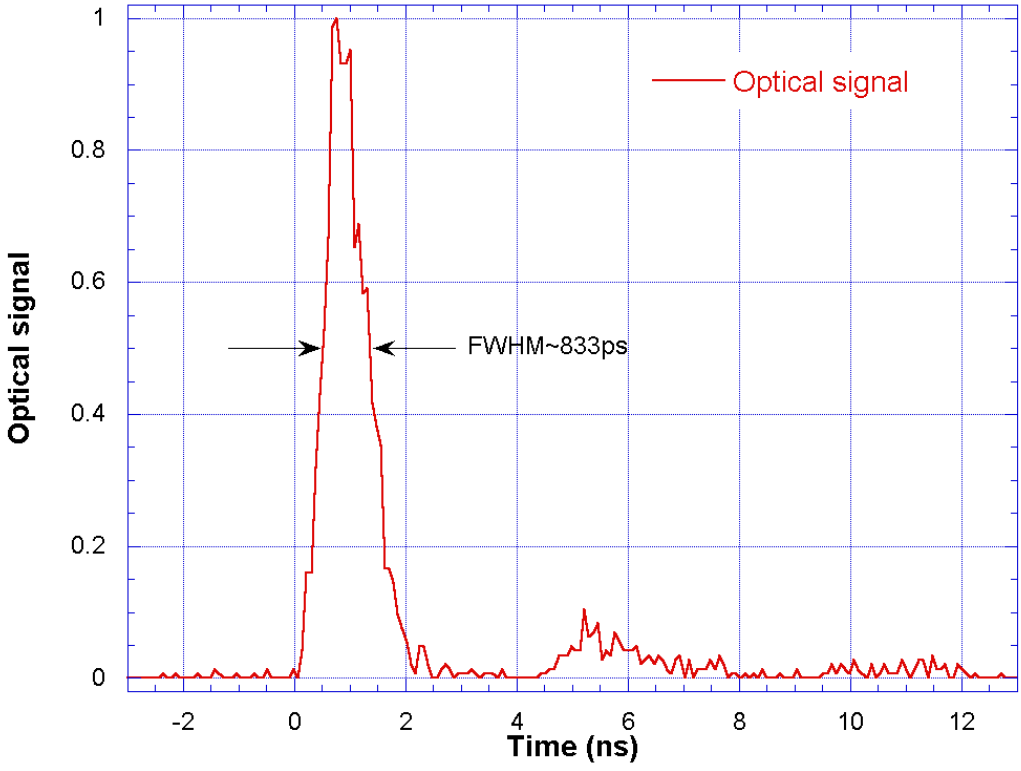


*Figure 7.22. Graph showing the optical pulse output from RCLED no1.*

The trace shows how the RCLED responds optically to the exciting pulse. An optical pulse of roughly Gaussian shape and 833ps duration (FWHM) is produced. A small afterpulse may be seen to the right of the trace. It is likely that this is due an electrical pulse reflection arising from an impedance mismatch in the driver circuit.

The amplitude of the after-pulse is small and would be further attenuated in a real system such that its contribution to errors or background count is negligible. Furthermore, any photons from the after-pulse would arrive at the detector at least 2ns after the main pulse and would therefore arrive outside of the nominal 1.4ns timing gate in use by the detector system. Such a pulse response shows the RCLED device has sufficient bandwidth and is ideal for use in the QC system.

#### *7.3.3.2 Narrowband filtering and RCLEDs.*

The discussion above yields two main points:-

- Firstly, the RCLED devices emitted a peak intensity at a wavelength nearly 12nm from the optimum required for maximum transmission through a narrowband filter situated at the 656.28nm Fraunhofer line. This is in spite of the design wavelength being quoted as 650+/-10nm.
- Secondly the RCLEDs are capable of producing very fast pulses. It is possible that the pulse width of 833ps shown in Figure 7.22 is not limited by the RCLED device but by the drive pulse. Therefore it is not unreasonable to suppose that even shorter pulses may be possible with this technology.

The wavelength shift may simply have been due to manufacturing tolerances, and, when questioned, the manufacturer stated that the emission from the RCLED devices could be engineered to coincide with the Fraunhofer line.

Normally it would be possible to temperature tune the sources to coincide with the filter transmission curve, but in the case of RCLEDs the output wavelength is constrained by, a resonant cavity. This has the effect, when temperature tuning the devices, of reducing the output intensity. The effect occurs because the gain-bandwidth of the material (the broadband emission one would expect from the material if it was used, say, in an ordinary LED) is shifted with temperature beyond the range of emission wavelengths that are allowed by the resonant cavity, which is short enough to allow only one cavity mode to propagate (compare this with lasers where the cavity is much longer and can support several modes). Figure 7.23 below shows the spectral behaviour of a production RCLED undergoing spectral analysis whilst being heated. There are three traces taken at three arbitrary temperatures. The temperature is not given, but the important thing to notice is that unlike laser diodes and LEDs, the spectral envelope does not shift appreciatively and the intensity drops as the gain bandwidth of the material moves away from the resonant frequency of the cavity.

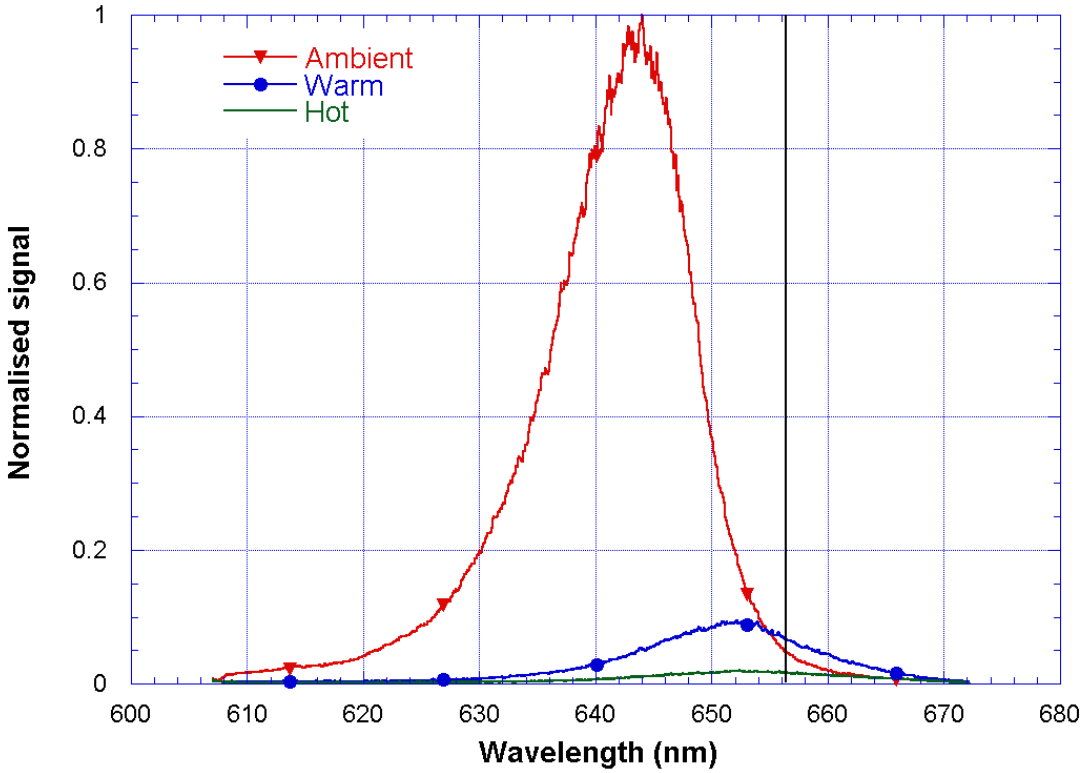


*Figure 7.23. Emission spectra from RCLED no9. when heated from ambient temperature. Ambient to hot is approximately 50$^{o}$Celsius. The 656nm Fraunhofer line is shown in black.*

The result is that at the desired wavelength, the intensity is even less than if the RCLED device was left unheated. If, however, the device is unheated then narrowband filtering will result in a significant loss of intensity due to spectral mismatch of the source and the filter. The situation is shown graphically in Figure 7.24. On the left one can see a plot of the normalised output from the RCLED against a plot of the filter transmission.

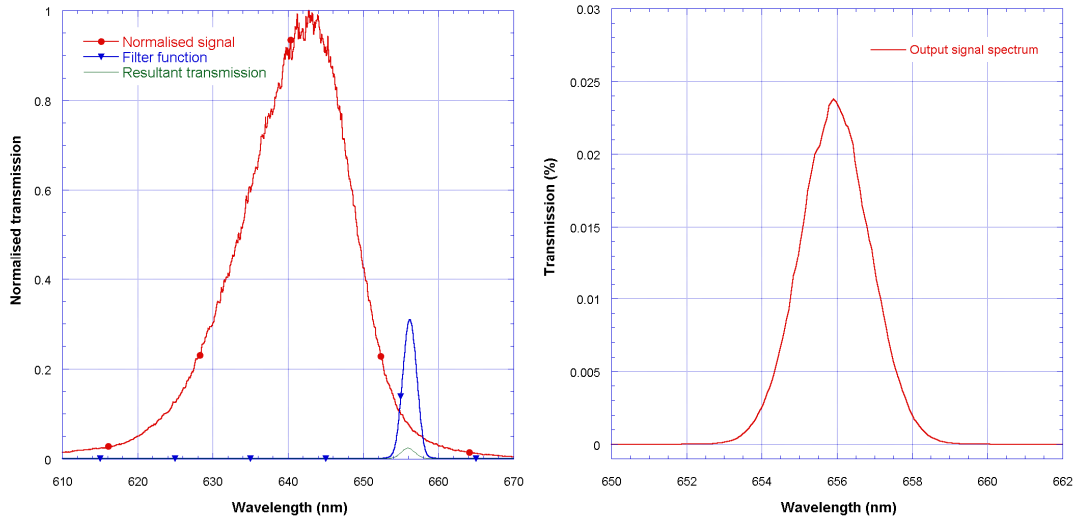


*Figure 7.24. Graph showing normalised output spectrum of a RCLED and narrow band filter. The resultant transmission is barely visible. For clarity, the resultant is shown enlarged in the graph on the right showing a peak transmission of 0.025%.*

It is possible to make a good estimate of the output of the device when filtered by the narrowband filter by multiplying the normalised signal and the filter transmission function. Although barely visible in the graph on the left, the resultant transmission has been enlarged in the graph on the right. Peak transmission is approximately 0.025% which is a loss of approximately 36dB. This is an extremely inefficient source.

In spite of this, four of the brightest (at 656nm) RCLED sources were selected and installed in the system. With the other optical components installed it was found to be only just possible to align the system. Unfortunately, too few counts were received (200 counts above background) to perform any key exchanges.

The results were considered encouraging providing that RCLED sources at the correct wavelength can be procured.

### *7.3.4 Spectral filtering*

Narrow band interference filters are a common tool in optical systems for selecting a narrow spectral band of light with the aim of increasing signal to noise ratios. A large number of filters are available with a typical spectral bandwidth of 10nm, and indeed filters with a central wavelength of 670nm and a 10nm bandwidth have been used as standard in the QinetiQ compact QKD system. Cost effective filters with a bandwidth less than 10nm are more specialised and difficult to obtain at custom wavelengths.

However, the chosen wavelength for daylight operation is the Hα line at 656.3nm for which narrow bandwidth filters are readily available. These have a nominal bandwidth of 1nm with a tolerance of 2nm. Using a very narrow band filter at this wavelength places a demanding requirement upon the emitting source to stay within the transmission band (see discussions of sources above), but also there are implications for the design of the collection optics.

The Bob receiver optical system discussed previously is shown schematically in Figure 7.25 below. The system consists of a long focal length (125mm) lens (50mm diameter) which focuses light through a 100μm diameter pinhole (acting as a spatial filter), onto another lens which images the incoming light onto the Bob detectors. The spectral filter is placed before the pinhole in a region where light is being focussed. It is well known that the spectral transmission characteristics of an interference filter are designed for use with collimated light, incident normal to the filter surface.

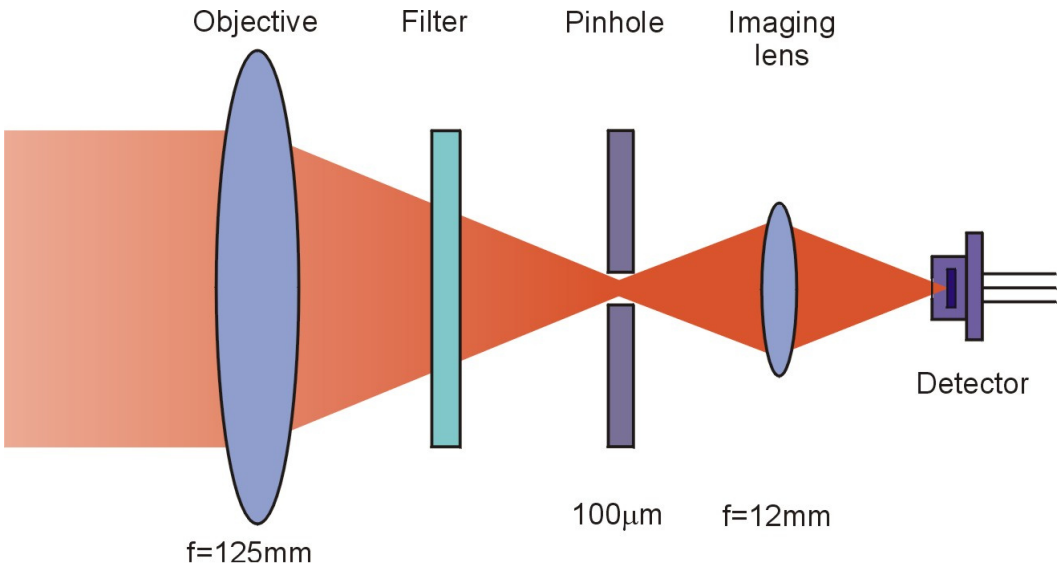


*Figure 7.25. The existing Compact QKD optical system for Bob at 670nm*

When light passes through the filter at an angle the central transmission wavelength shifts to shorter wavelengths [10]. This effect is shown in Figure 7.26. A 650nm filter transmission function is shown for normal and $10^{o}$ off-normal incidence. The transmission maximum for off-normal radiation moves to shorter wavelength by approximately 5nm and results in a transmission reduction of nearly 15% at the 650nm peak compared to collimated light.

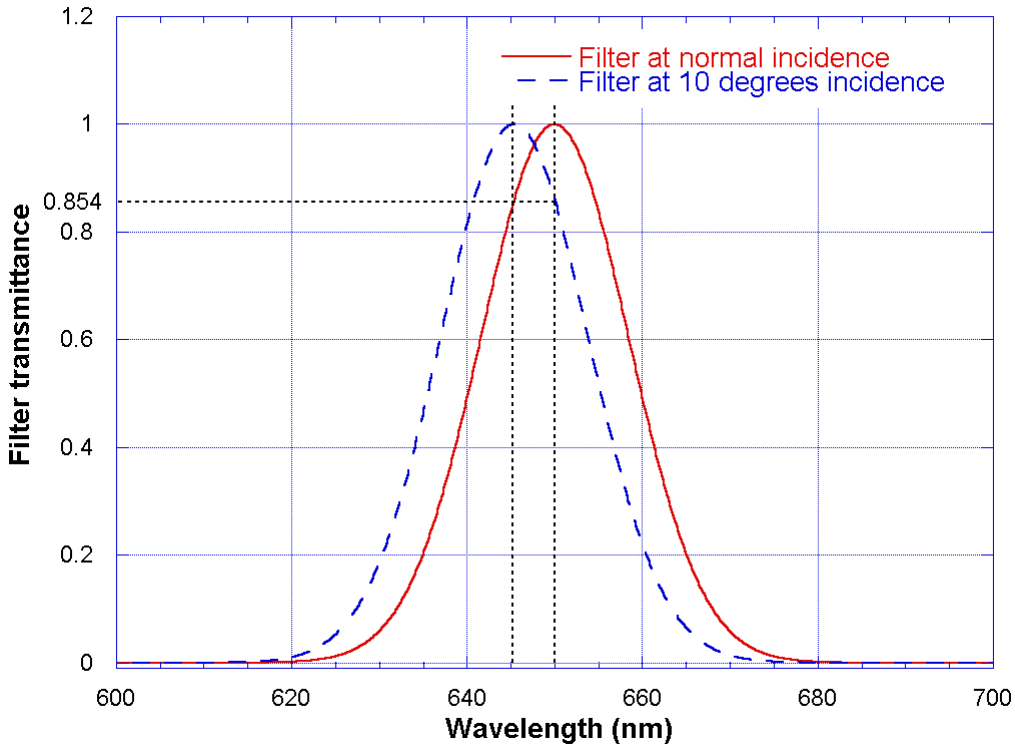


*Figure 7.26. Spectral transmission profiles of an interference filter on axis (red) and 10° off-axis (blue dashed). Peak transmittance shifts by approximately 5nm to shorter wavelength.*

With a narrower bandpass filter the transmission loss would be significantly increased. Furthermore this loss affects only the signal wavelength as the background radiation possesses a broad spectrum and therefore always has a component with transmittance in the pass band of the filter. The effect of off-axis transmission is therefore to reduce the signal to noise ratio. A method of alleviating this problem would be to mount the narrow-band filter at a point where the incoming light is collimated.

### *7.3.5 Field of view (FOV) considerations*

The field of view (FOV) of a system is the angle over which the optics of the system is able to accept light. The amount of light collected by a system is thus determined by the FOV and any stops in the system. For clarity, a simple optical system is shown below.

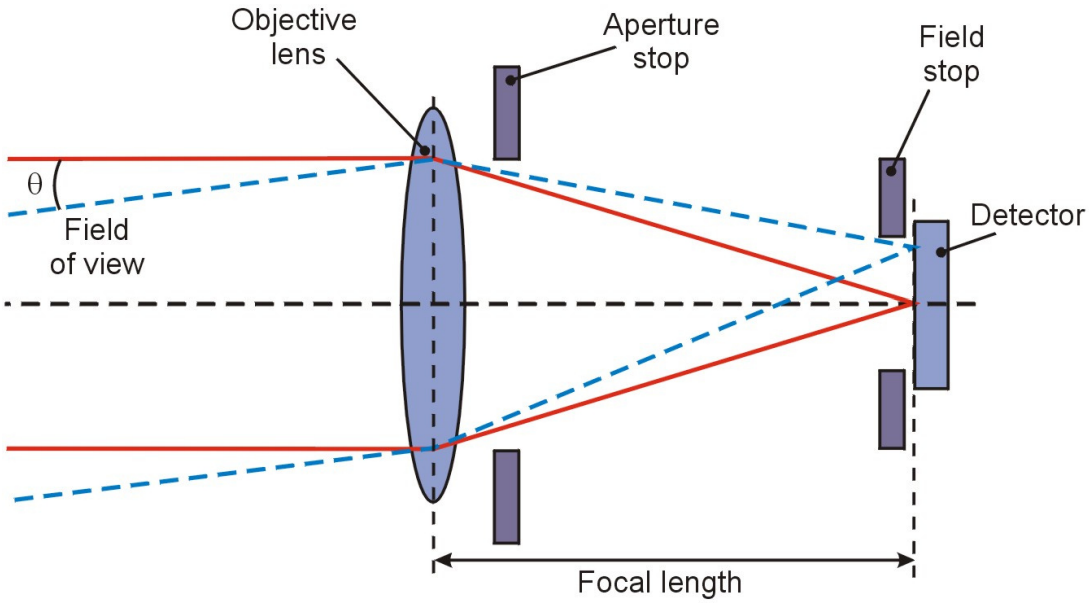


*Figure 7.27. Simple optical system showing aperture and field stops and the field of view.*

Clearly, the FOV of the optical system can be controlled by a number of methods such as entrance aperture, focal length, aperture and field stop sizes. Significant background reduction could be made by restricting the field of view of the receiver to a small angle and thus accepting light from as small an area as possible around the Alice output lens.

#### *7.3.5.1 Use of a field stop*

The QinetiQ compact QKD system employs a 100μm diameter pinhole situated at the focus of the collecting lens as a field stop (see Figure 7.25. above).

Whilst this arrangement blocks a proportion of the scene image from reaching the detector, it is not necessarily the correct proportion since the pinhole is positioned at the focus of the objective (i.e. the Fourier plane).

The pinhole thus acts as a spatial filter and only light of lower spatial frequencies is passed. This light could still contain elements from the wider scene around Alice. Moreover, since the light being gathered by the system has inevitably passed through the atmosphere and become distorted in various ways, it may well contain desirable higher spatial frequency elements which are being filtered. A better way of filtering would be to employ a field stop at a location closer to the objective thus enabling a reduction of the image field.

#### *7.3.5.2 Focal length increase*

It is clear from Figure 7.27 that the background level can be reduced through the use of a longer focal length collection. The amount of light collected varies as the inverse square of the focal length, so doubling the focal length reduces the light collection by a factor of 4.

However the focal length of the lens system cannot simply be extended arbitrarily because the physical size and weight of the telescope optics would make the system impractical. A sensible approach would be to use a catadioptric folded optical system such as a Schmidt-Cassegrain reflecting telescope. This type of system is physically small but has a long focal length and would alleviate possible problems with centre of gravity and bulk etc. Such a system has a small disadvantage in that the telescope has a central obscuration, however, this can be offset by slightly increasing the aperture size.

### *7.3.6 Revised optical system*

With the above in mind, a new optical system for the Bob receiver was designed. A commercial of-the-shelf Schmidt-Cassegrain telescope with a focal length of 500mm was procured and coupled to suitable mountings. The new optical system for the Bob receiver is shown schematically in Figure 7.28.

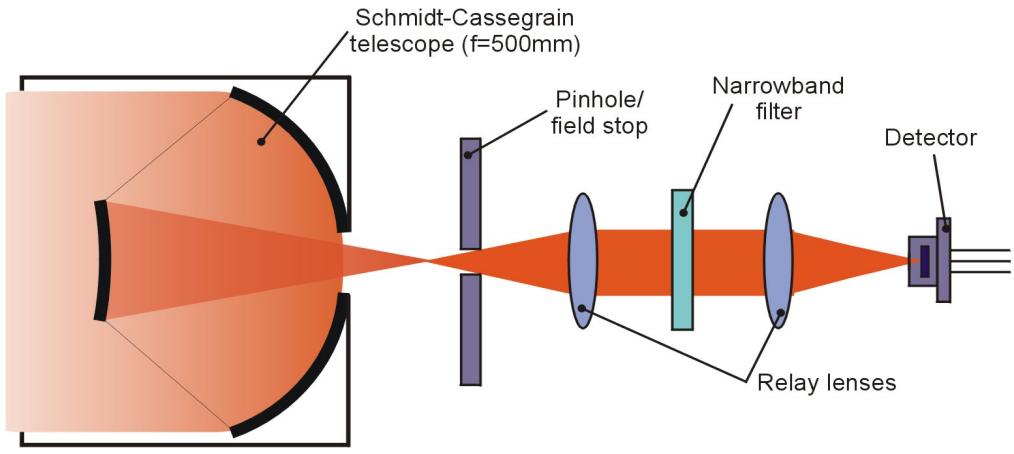


*Figure 7.28. A schematic diagram of the new optical system for Bob, incorporating a Cassegrain reflecting collector.*

The redesigned collecting system possessed an F-number of 8 and a focal length of 500mm with approximately twice the collection area of the previous system. This made the system more efficient at collecting both background and signal and thus did not affect the signal to noise ratio. However, the increased collection efficiency makes more light available to the filtering elements later in the system. A feature of the new collection lens (and of Schmidt Cassegrain systems in general) is the central obscuration of the collection aperture. This was found to create problems at short ranges where a mismatch between beam sizes meant that the whole beam was obscured necessitating the use of a skewed optical path. This was not expected to cause problems at longer ranges and the resulting larger beam diameters.

A smaller pinhole (75μm) was installed as a field stop. Although significantly smaller than the original 100μm pinhole, this is still much larger than the expected focal spot created by the objective lens. However, for the reasons stated above the pinhole should act as a field stop and not necessarily as spatial filter and therefore is required to be somewhat removed axially from the focal plane of the objective and larger than the focal spot. Another reason for a conservative choice of pinhole is that the smaller the pinhole, the more sensitive to alignment the system becomes. This is compounded by increasing the focal length of the system. Obviously there is a trade-off to be made with implications for the design of the mounting and pointing systems. Finally an additional relay lens was installed thus creating a region of collimated light for the optimum installation of a narrowband filter.

Due to the difficulties in directly comparing the old and new systems it was decided to make progressive change to demonstrate that the suggested changes would be effective.

### *7.3.7 Jitter, gating, and noise*

The Alice transmitter emits pulses at a fixed rate with a fixed time interval between pulses. The QKD system is synchronised such that propagation delays are removed from the photo-detections made at the receiver and therefore Bob can unambiguously predict the arrival times of specific pulses. In practice, the time of arrival of the emitted pulses exhibits a statistical spread which originates from various sources such as atmospheric effects and electronics noise. This spread is called jitter and it places a limit on the system performance. Figure 7.29 below shows a typical histogram of signal detections at the receiver.

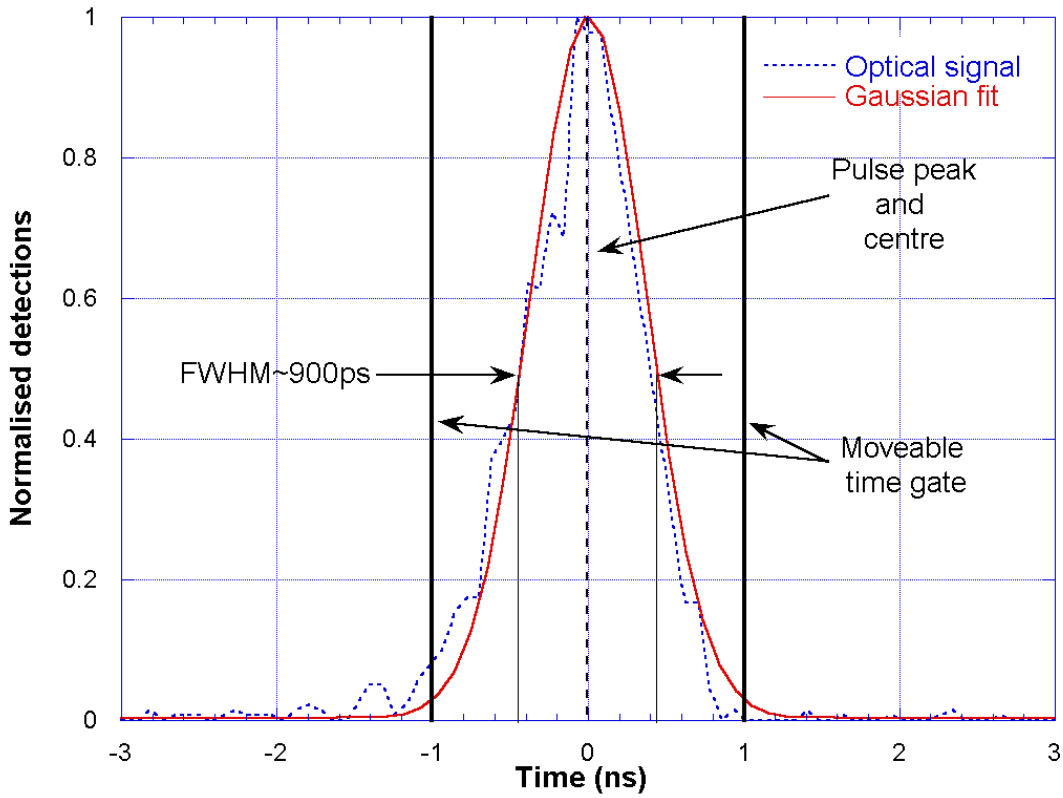


*Figure 7.29. A typical detection histogram from a QKD receiver (blue dotted), with a Gaussian fit (red solid). The moveable gates determine how much of the signal pulse (and background) enter the detection system.*

The histogram above depicts a normalised set of photo-detections lying squarely within a detector gate (a Gaussian approximation is also shown for convenience). Detections lying outside the gate are regarded as noise and ignored. However, because such noise events occur randomly, there is a finite probability that they will fall within the gate and result in an erroneous count. This probability is proportional to the gate width and so it is important to use a gate width as narrow as possible.

Obviously, if the gate is reduced too far a loss of signal will result. If now the gates are now bought incrementally together, clearly less of the signal will lie within the gate. This situation is show below in Figure 7.30.

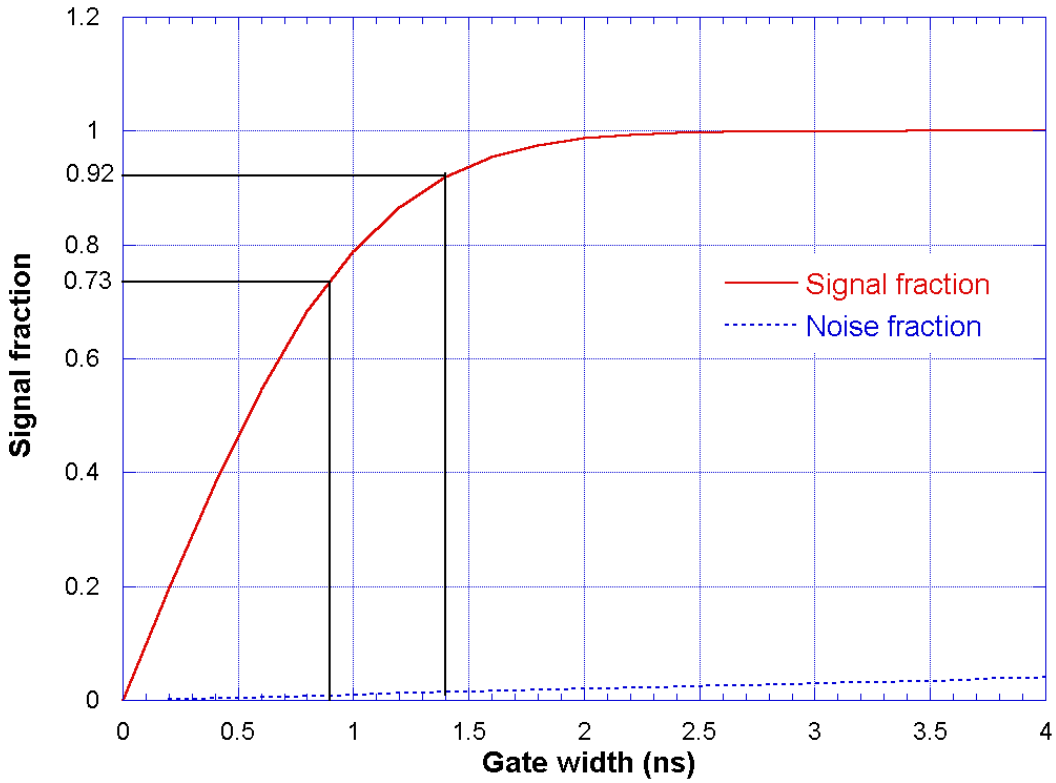


*Figure 7.30. Graph showing the fraction of signal (red continuous) and noise (blue dotted) contributing to the raw key as a function of timing gate width.*

Clearly, with reference to the plot above, there is little to be gained from reducing the width of the time gate below approximately 2ns since this would reduce signal at a greater rate than the background noise contribution. The full width half maximum of the pulse in this example is approximately 900ps, therefore for maximum signal one would open the gate for approximately twice this value.

### *7.3.8 Background reduction results.*

To demonstrate the effect of the modifications discussed above on the receiver system background rejection performance, several tests were performed.

In the case of the spatial filter/field stop, a filtered Bob receiver without a collecting lens was placed facing a white, evenly illuminated diffuse reflecting surface. The background count level was then measured. The effect of various pinhole sizes on background may be seen below in Table 7.3.

| Pinhole Diameter (μm) | Filter (nm) | Count rate (kHz) | Reduction factor | Expected reduction |
|---|---|---|---|---|
| 100 | 10 | 126 | 1.0 | 1.0 |
| 75 | 10 | 76 | 1.67 | 1.7 |
| 30 | 10 | 12 | 11.1 | 11.1 |

*Table 7.3. Count rate reductions from reduced diameter pinholes.*

The reduction in background delivered by the pinhole size adjustment is clearly consistent with the expected result (that is a square law relationship).

Comparison of filter efficiency was then made by replacing the 10 nm bandwidth filter with one possessing a transmission band of approximately 1nm. Three filters, nominally the same, were installed in turn and background count rates again measured. The results are shown below in Table 7.4.

| Filter (nm) | Pinhole (μm) | Count rate (kHz) | Reduction Factor | Expected reduction |
|---|---|---|---|---|
| 10 | 100 | 350 | 1.0 | 1.0 |
| 1 (filter 1) | 100 | 57 | 6.25 | 10 |
| 1 (filter 2) | 100 | 45 | 7.8 | 10 |
| 1 (filter 3) | 100 | 54 | 6.7 | 10 |
| 1 (filter 1) | 30 | 4 | 91 | 111 |

*Table 7.4. Count rate measurements for reduced bandwidth filters and selected pinholes.*

The pinhole size reduction (30mm) shows an improvement in background collection by an order of magnitude whilst the new filters showed a reduction in transmitted count rate of approximately a factor of 6. The final result in Table 7.4. shows the system with a 30μm pinhole combined with a 1nm filter giving an overall reduction in background by a factor of 91, somewhat less than the anticipated reduction. However, the above measurements show that the suggested improvements in reducing both pinhole size and filter band-pass width behave in a manner consistent with the expectations.

### *7.3.9 Extended daylight operation trial*

Due to the difficulties experienced with attempts to implement a broadband RCLED source combined with a narrowband filter, the system was constructed using semiconductor laser diodes emitting at approximately 656nm. The other improvements discussed above were included in the new design and resulted in an overall reduction in background of approximately 25dB. Although not the required 30dB reduction this figure is encouraging and sufficiently low to enable key exchanges to take place.

The system was located in a well-lit (both natural and electric) laboratory with the Alice transmitter located in front of a large window such that the Bob receiver was looking into a bright daylight scene. The system was then set to run continuously in an autonomous batch mode with each batch consisting of 100 blocks of data.

Here, a block of data consists of a header component containing a pseudo random bit sequence (PRBS), used to synchronise the two terminals, followed by random data component containing $20\times10^6$ pulses. A complete batch transmission was accomplished approximately every 200 seconds.

If, for any reason, a block synchronisation fails, the system waits until the next block and tries again. At the end of each batch, key reconciliation occurs with Alice and Bob performing a complete reconciliation of the exchanged key. During this phase the key material is stored, along with information about the statistics of the process, such as the number of valid blocks received and the bit error rate for the batch as a whole. With the batch reconciliation complete the process is repeated for the next batch.

#### *7.3.9.1 Results*

The system was left to run continuously for 7 days without any intervention and several system parameters were recorded. The resulting key and error rates are shown below in Figure 7.31. This work is also reported in [11].

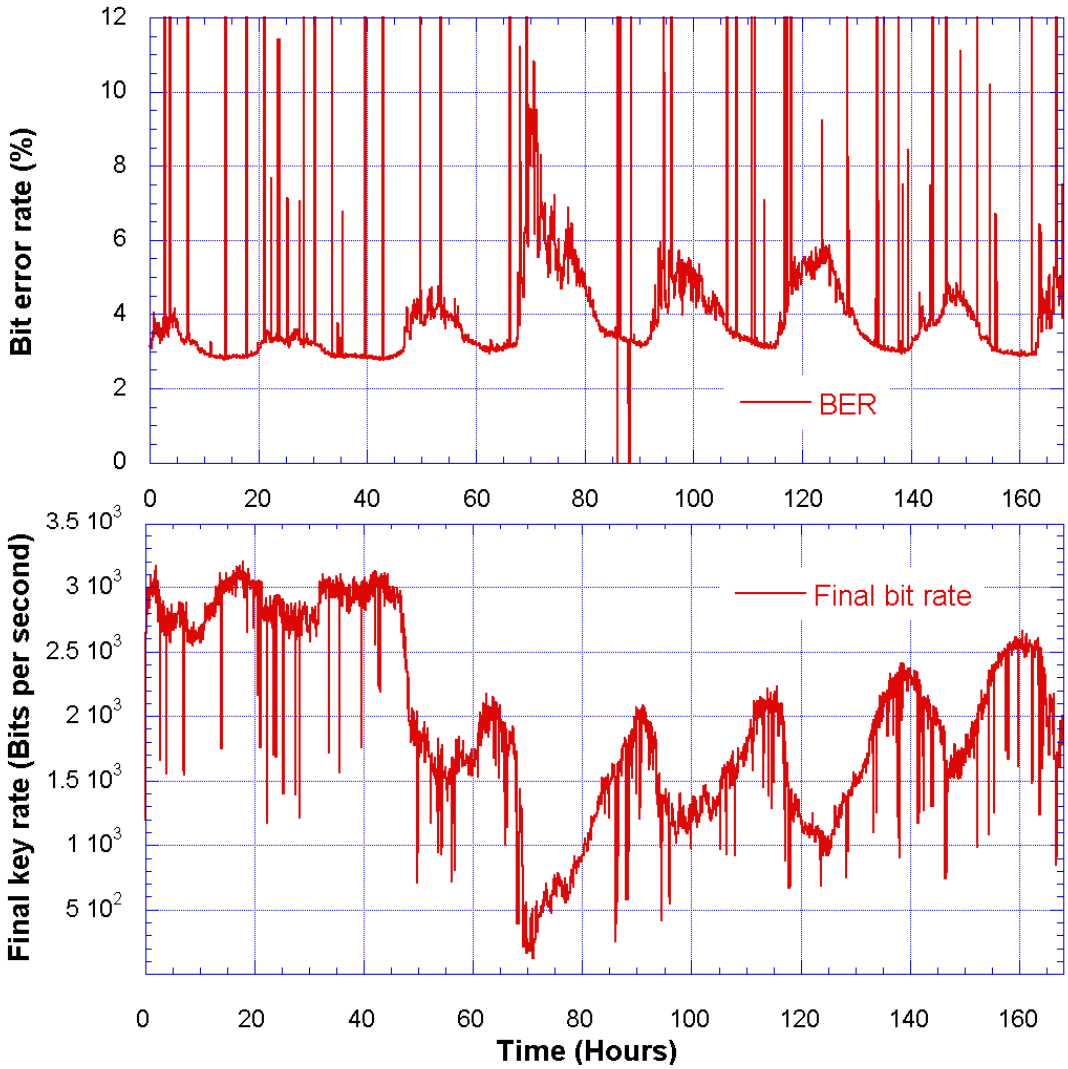


*Figure 7.31. Graph showing final key rates and bit error rate over 7 days of operation of the daylight enabled system, using modified Cascade error correction and privacy amplification algorithms as described in section 7.3.10.3 below.*

Firstly, it is easy to see the matching diurnal variations in both key and bit error rates. Also, around the 50 hours mark, the system appears to suffer from a significant

reduction in efficiency with a corresponding increase in error rate, during both day and night hours. This is probably due to a misalignment in the system due to a temperature fluctuation in the laboratory.

The spikes of higher QBER arise from occasions when the synchronisation has failed for a large number of blocks within the batch. In general the spikes last for a single batch after which the system recovers. Shared key is generated from each individual block, so even where the average batch QBER may be high, there may be some good blocks with low QBER that can yield key. It is clear that synchronisation failure occurs most often during the daylight hours.

At the end of each batch the value of μ, the average photon number per pulse was measured using an amplified photodiode located at the unused output port of the combining beamsplitter in the Alice transmitter. A narrow bandwidth spectral filter of the type used in Bob was placed in front of the photodiode. The photodiode output is shown below.

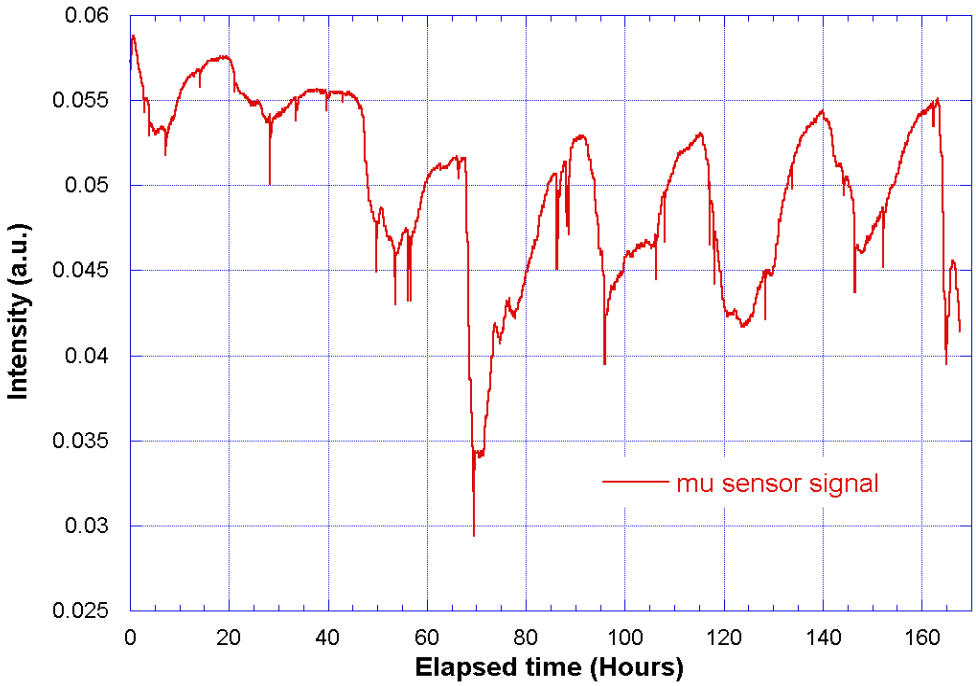


*Figure 7.32. Graph showing output intensity of Alice during the experiment.*

Due to the photodiode location, the output intensity value was not influenced by system alignment due to thermal fluctuations, or to the influence of varying degrees of background radiation.

Therefore, the most likely source of the variations in figures 7.31 and 7.32 is fluctuations in the overall transmittance of the laser beams due to thermally induced changes in the emission wavelength of the semiconductor lasers causing a mismatch between the laser output wavelength and the filter passband.

With a QBER rate of 3-6% and final key generation rates of 1-3 Kbits per second the system performed well although this experiment was performed over a few metres in a laboratory. However, atmospheric loss was simulated by using neutral density filters at the transmitter in an attempt to yield losses typical for systems in use over several kilometres.

### *7.3.10 General development work*[13]

In addition to the modifications described above, several areas were identified as having a significant effect on system performance.

- Pointing and alignment
- Continuous operation
- Algorithm improvement.

A brief description of development work in each area is given below.

#### *7.3.10.1 Continuous operation*

Previous versions of the compact QKD system software were designed to process data in a packet mode characterised by sending blocks of random key material prefaced by a pseudo-random header. Sifting, error correction and privacy amplification were then applied to each batch in turn before a final secret key was produced. The process was then repeated on a batch by batch basis and was necessarily discontinuous in nature. A new version of the software was written that allowed key generation to take place continuously. The software was developed to conduct the separate phases of key generation, including key reconciliation, in parallel and to generate random key until stopped by the user. The continuous QKD system was then operated for 24 hour in a laboratory test. The results are shown in the graph below in Figure 7.33.

The graph shows the received quantum key rate at Bob after the processes of detection, sifting and error correction. After what appears to be a settling period of a couple of hours, a stable key generation rate of approximately 3kBits per second is established. Also shown is a graph of the bit error rate of the transmitted data.

It is clear that the early lower QBER coincides with the higher key rates with the system settling after some hours. In order to service the increased demand for random numbers, the random number generator software was modified to continuously deliver real time random numbers to the system.

[13] This work was conducted as part of a four man team with contributions from every member. It should be seen as general work improving system reliability.

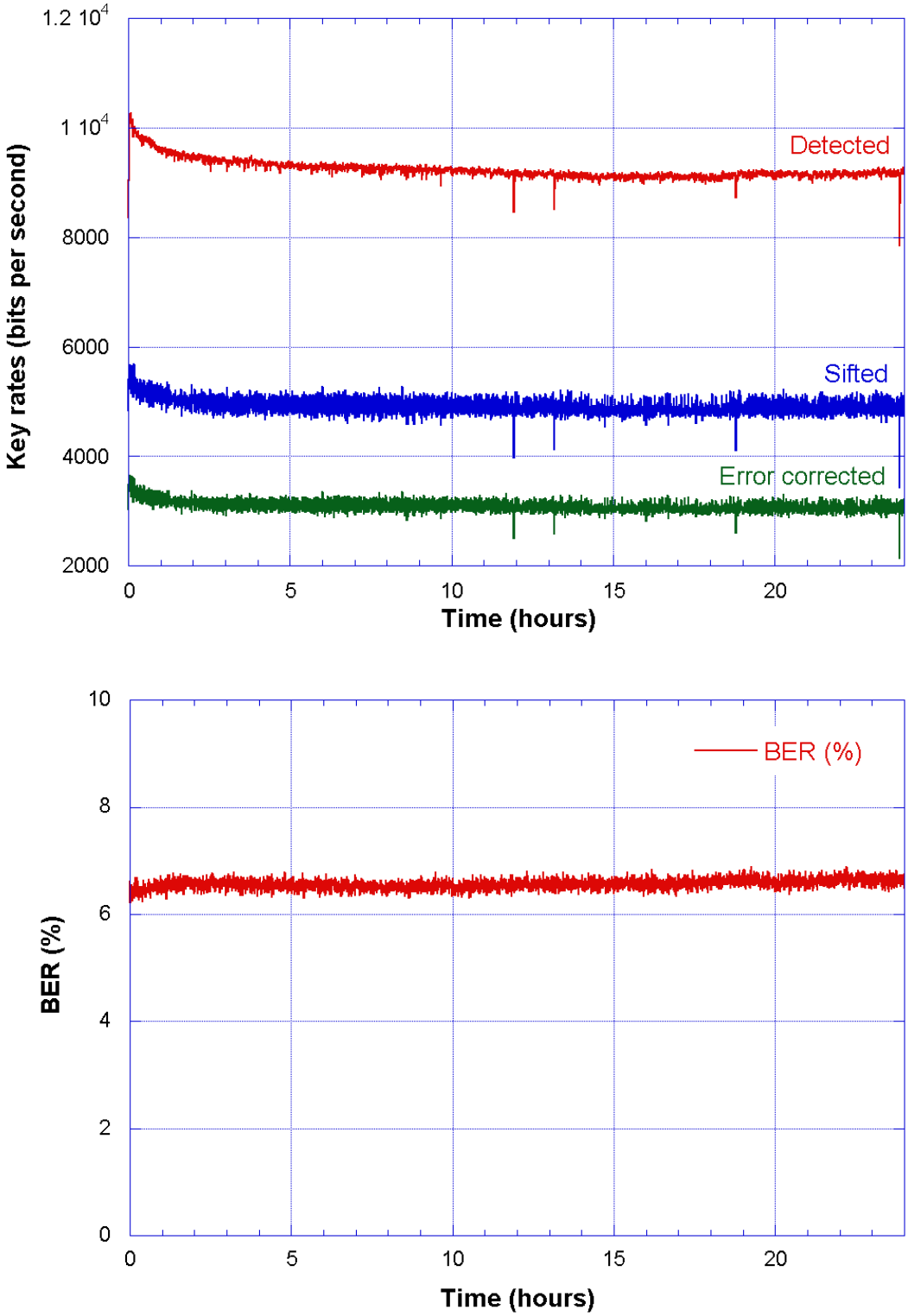


*Figure 7.33. Key generation rate and bit error rate for the continuous QKD system using modified Cascade error correction and Privacy amplification algorithms described below.*

### *7.3.10.2 Pointing and alignment.*

It has long been recognised by the QKD community that accurate pointing and alignment are extremely important, particularly for free-space systems operating over more than a few hundred metres.

With this in mind, it was decided to install a pointing and tracking system into the compact QKD system. A pair of miniature video cameras were installed in the system and connected via USB cable to the controlling computer. The cameras were coupled into the optical beam using suitable beamsplitters such that fields of view of the transmitter, receiver and their respective cameras were co-aligned and boresighted.

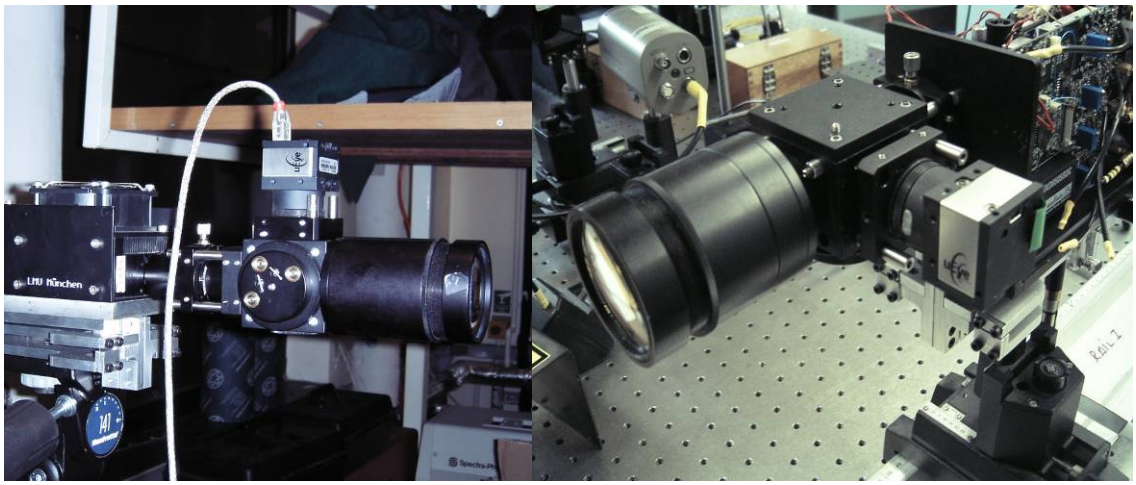


*Figure 7.34. Alice and Bob modules showing output optics with miniature USB video cameras attached.*

This arrangement allowed the operators to see exactly where each optical system was pointing at any given time. With the system aligned, fiducial marks were overlaid on the video display such that subsequent re-alignment was merely a matter of aligning the marks. Both transmitter and receiver systems were also provided with a set of motorised micrometers for fine pan and tilt adjustment. A simple tracking routine was then written in LabVIEW to enable the system to compensate for small drifts in alignment.

#### *7.3.10.3 Algorithm improvement*[14]

In addition to the improvements detailed above, much time was spent improving the efficiency of the Cascade error correction algorithm. In order to make best use of the classical link hardware, the key was divided up into a large number of blocks, and a parallel Cascade process was implemented.

This means that the cascade algorithm is implemented separately and simultaneously on each of the blocks. During this process the erroneous bits are publicly revealed, together which a few extra bits used in the isolation process.

At the end of the cascade algorithm the corrected key is shortened, so that the eavesdropper has no information on what remains.

[14] This unpublished work was exclusively and exhaustively undertaken by Paul Tapster. I include it here as it was part of the final system. It is also a significant result in its own right.

This can always be done with perfect efficiency; (i.e. the number of bits removed is equal to the number of bits revealed during error correction).

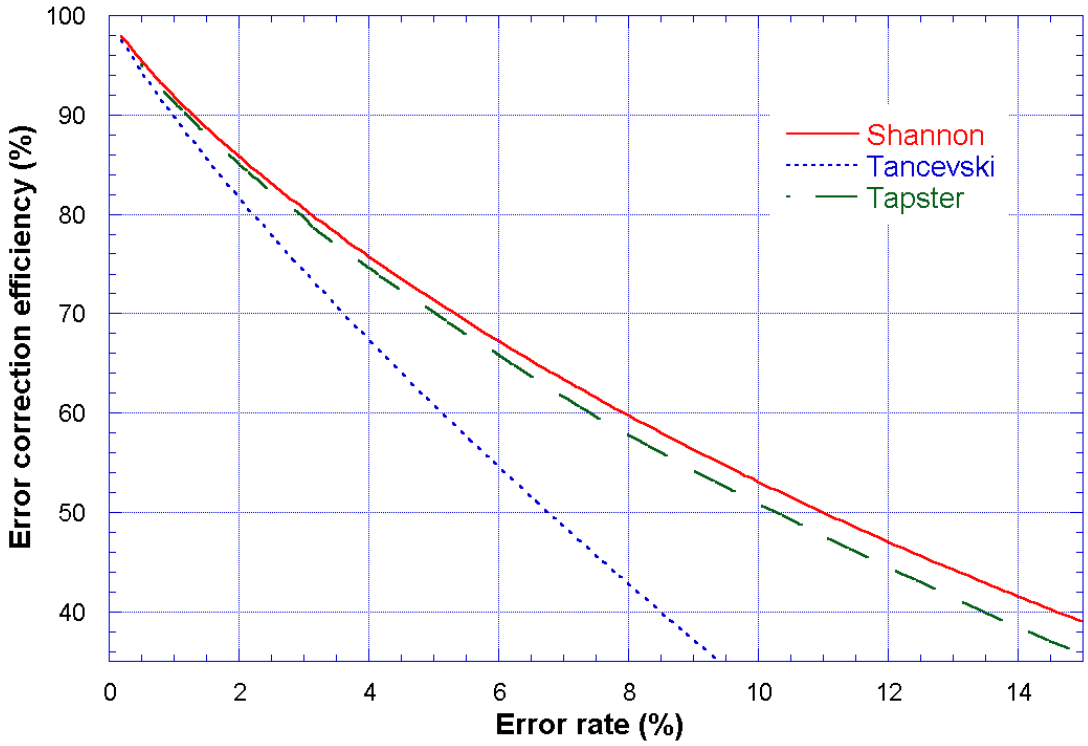


*Figure 7.35. Comparison of error correction efficiencies showing the Shannon limit (best case), Tančevski's estimation of Bennett and Brassard's Cascade and Tapster's version of Cascade with parallel processing.*

The diagram in Figure 7.35 shows the efficiency of the version of the algorithm that was used in the compact QKD system (middle-dashed curve) together with the maximum theoretical efficiency (upper-solid curve). For comparison the estimation by Tančevski of the efficiency of the original Cascade is shown for comparison (lower-dashed). Clearly, Tapsters algorithm is not only an improvement in terms of efficiency but also robustness against higher errors, reaching to within a few percent of the Shannon limit.

## 7.4 Daylight operation conclusions

Attempts to reduce the background count rate of the compact QKD system by several means have been described in some detail. When comparing the modified optical system (500mm focal length, 1nm filter and a 30µm pinhole), against the original system (125mm focal length, 10nm filter and a 100µm pinhole) a reduction in background of approximately two orders of magnitude was noted.

An anticipated improvement of 3 orders of magnitude could not be achieved by these means alone and the reason for this discrepancy is unclear.

Increased narrowing of the timing gate was not attempted for the reasons given above in section 7.4.3. However, future reduction in transmitter pulsewidth and system jitter would allow the time gate to be reduced thus reducing the background probability accordingly.

Attempts were made to align Alice and Bob incorporating the new background reduction features but the increased alignment sensitivity due to a greater level of magnification, coupled with the restriction presented by the reduced pinhole made alignment difficult and unreliable.

A detailed discussion of sources for daylight QKD operating in the 656nm Fraunhofer line showed some promise for RCLED devices in a future system although the test devices were unsuitable due to wavelength.

The system was demonstrated over several days in a daylight scenario and also in a continuous mode generating secure key material at rates up to 3kbits per second.

## 7.5 Chapter 7 references


[1] J.G. Rarity, P.M. Gorman and P.R. Tapster, “Secure key exchange over 1.9 km free-space range using quantum cryptography”, Electronics Letters **37**, 8, 512, (2001).

[2] R. J Hughes, J. E. Nordholt, D. Derkacs and C. G. Peterson, “Practical free-space quantum key distribution over 10 km in daylight and at night”, New J. of Phys. 4, 43.1–43.14, (2002).

[3] H. Weier, T. Schmitt-Manderbach, N. Regner, C. Kurtsiefer and H. Weinfurter, “Free space quantum key distribution: Towards a real life application”, Fortschr. Phys. **54**, 8 – 10, 840 – 845, (2006).

[4] D. J. Rogers, J. C. Bienfang, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, L. Ma, D. H. Su, Carl J. Williams, and Charles W. Clark, “Free-Space Quantum Cryptography in the H-α Fraunhofer Window”, Free-Space Laser communications VI, Proc. of SPIE Vol. 6304, 630417, (2006).

[5] Table reproduced from "Astrophysical Formulae", edited by K.R. Lang, Springer Verlag, p175, (1978).

[6] Joseph Reader, “Reference Wavelengths for Strong Lines of Atomic Hydrogen and Deuterium”, Applied Spectroscopy, **58**, 12, (2004).

[7] D. Delbeke, R. Bockstaele, P. Bienstman, R. Baets, and H. Benisty, “High-Efficiency Semiconductor RCLEDs, A Review”, IEEE Journal on Selected Topics in Quantum Electronics, **8**, 2, (2002).

[8] J. D. Lambkin, T. McCormack, T. Calvert and T. Moriarty, “Advanced Emitters for Plastic Optical Fibre”, White paper for Firecomms Inc, (2002).

[9] Firecomms FC300R-120 High speed Resonant cavity LED Datasheet. URL: http://www.firecomms.com/downloads/datasheets/FC300R.pdf, (2007).

[10] R. M. Lerner, “Limitations in the Use of Dielectric Interference Filters in Wide Angle Optical Receivers”, Applied Optics, **10**, 8, (1971).

[11] D. M. Benton, P. M. Gorman, P. R. Tapster and D. M. Taylor, “A compact free space quantum key distribution system capable of daylight operation”, Optics Communications, **283**, 11, 2465-2471, (2010).

# Chapter 8- Conclusions and future work

## 8.1 Conclusions

This thesis has presented the author's work on free-space QKD systems performed at QinetiQ (Malvern) and its predecessors over the period of a decade from 1998.

Chapters one to four have introduced the field of quantum key distribution and some related areas and given a historical review of the technology. In addition, the theoretical basis has been presented along with the necessary theoretical tools for understanding some of the practical problems associated with implementation of the technology

Chapters five to eight have presented practical work in free space QKD performed by the author and co-workers starting from a breadboard proof of principle system through to a compact, reliable and portable system, elements of which have been demonstrated over distances up to 144km and in daylight.

The key results of the research is that free-space QKD is a versatile and robust technique for exchanging highly secure encryption keys in certain scenarios such as short haul metropolitan and long haul (low earth orbit) links.

### *8.1.1 Lessons learned*

It is easy, in a small team, to become so focussed on the current research topic that one misses important developments in the field. This became apparent when comparing our system results against the current security proofs. Most of the QinetiQ results fail to stand up against a rigorous security analysis using the latest theory. However, this can often be attributed to the fact that theoretical QKD development appears to have lagged that of practical systems for much of its life. A greater awareness of current security proofs by the team would have resulted, for instance, in a much earlier development of a Decoy State protocol for the compact system.

Of course, this is not to say that the QinetiQ system is not as vulnerable as any other system to an as yet unknown side channel attack or hack. The group at Trondheim (V. Makarov and colleagues) appear to be the only group seriously attempting the task of subverting QKD systems.

## 8.2 Future work plans at QinetiQ

Subsequent to the end of the UKMoD program which funded much of the work described in this thesis, the QinetiQ team was refunded for a further three years to study and develop components for QKD systems. The new project focussed on developing the fundamental technical building blocks using robust and reliable GaAs solid state technology for the next generation of QKD addressing security at higher data speeds and with wider application areas. This project aimed to develop two device technologies:

***A high-speed optical polarisation modulator*** – The first technology builds upon technology arising from an earlier programme for QC development [1]. A waveguide-based device capable of rapidly modulating the polarisation of its output light is of enormous potential value to so called weak pulse QC systems. It is capable of generating all the polarisation states required for the implementation of QC protocols using a single laser, as opposed to current systems which use multiple sources. In addition it can also be used to compensate for polarisation scrambling effects such as those found within optical fibres. The use of low voltages and high speed shows potential for wider usage in telecommunications systems. The newly funded work seeks to refine the device design described in [1] and extend the modulation rate from 100 Mbit/s to 10 Gbit/s. This will greatly enhance QC key distribution rates as well as being of benefit to conventional optical telecommunications, enabling the future demands of secure data transmission volumes to be met.

***An entangled photon pair source*** – involves the development of a novel non-linear waveguide structure to produce entangled photon pairs with high efficiency in a compact and easily controllable form.

This technology [2] requires the design of a source of quantum mechanically entangled photons intended for use in a quantum cryptography system or quantum information systems. In quantum information in general (which includes QKD), entangled photons can be considered a resource. They can replace ‘weak pulse’ sources to create a type of single photon source, or they can be sent from a third party (which need not be trusted) to secure a key between two separated users. In each case they have the potential to increase data rates for the same level of security as weak pulsed systems. In addition, entanglement is a key technology in quantum repeaters (a proposed method of increasing the range of fibre optic based QC) and in optical quantum computation.

Most existing techniques for the generation of entangled photon pairs rely on relatively large designs with bulk optical components and laser systems.

This work aims to demonstrate novel phase-matching schemes for non-linear wavelength generation in structured semiconductor waveguides, with a view to enabling efficient generation of entangled photon pairs for QC. Novel gallium arsenide (GaAs) waveguide designs generate the non-linearity over an extended interaction length (yet in a compact space), permitting the required optical intensities to be achieved with relatively low pump laser power.

Additional research at QinetiQ is also focussed on development of a QKD network solution using a polarisation-based broadcast method over passive optical networks (PONs).

## 8.3 Future trends

***Global reach QKD:*** To date, the author is unaware of any QKD system that has been placed aboard a space vehicle or, for that matter, placed on any high altitude platform. This thesis has detailed some of the feasibility research during the past two decades but no practical realisations have been reported. Several groups are working toward this goal including the Hughes group at LANL in the U.S. and the Spacequest collaboration [4] based at the University of Vienna.

***Networked QKD:*** Network QKD is still in its infancy despite enormous efforts to develop various implementations. The most promising of which appears to be the broadcast P.O.N solution which does not require secure nodes in the network. Recent networked applications of QKD included a system securing some of the communications at the FIFA world cup in South Africa (2010)

***QKD to the home:*** With the advent of all optical networks and fibre to the user (FTTU) technologies it has become possible to perform QKD over passive optical networks right into the home or business. Compact technologies, such as waveguide modulators would allow the development of a cost effective solution for online security [6].

## 8.4 Outlook

The appearance of working QKD has attracted much interest. However, it appears that there is some reluctance to embrace the advantages of QKD commercially, but this is generally the case with new technologies. Typically, Far-Eastern countries such as Japan, China and Singapore appear to be investing heavily in QKD technology. Although there are still many problems to be solved, the potential gains may well make QKD a successful technology particularly in light of the threat to security posed by the increasing likelihood of a viable quantum computer.

## 8.5 Chapter 8 references


[1] E. D. Finlayson, P. M. Gorman, J. M. Heaton, M. J. Kane, B. S. Lowans, "Electro-optic waveguide polarisation modulator", UK Patent application number: GB 2441 790 A, (2008).

[2] D. M. Benton,; P. M. Gorman, P. R. Tapster, D. M. Taylor, E., D. Finlayson, "Non-Linear Optical Device", International patent Application No. PCT/GB2009/002745, (2009).

[3] Y. Zhao, Chi-Hang Fred Fung, B. Qi, C. Chen, and H-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems", Phys. Rev. A 78, 042333, (2008).

[4] Space quest at the University of Vienna: URL: http://www.quantum.at/quest, (2008).

[5] ID Quantique press release, URL:http://www.idquantique.com/news/press-release-worldcup.html, (2010).

[6] P. M. Gorman, D M Benton, P R Tapster, D M Taylor, E M Finlayson, "Quantum Cryptography hardware for the FTTX* end user", QinetiQ invention report no.034411. (July 2008).